“I think they mean it.” The new medical records privacy law in Texas

By B. Joyce Yeager, CIPP/US

Revisions to the Texas Medical Records Privacy statute, which take effect on Sept. 1, expand existing requirements for those who have access to medical information pertaining to others. House Bill 300 (HB 300) provides that covered entities, as defined in the statute, must comply with expanded responsibilities pertaining to health information. The act imposes upon these covered entities additional duties beyond those that are dictated by the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA). Because the state statute affords additional protections beyond those provided by HIPAA, no federal preemption issue should exist.

Penalties for failure to comply are substantial and include civil monetary penalties, the potential for loss of professional licensing and even the potential for state law criminal felony prosecution. Entities and individuals within the state who have access to medical information of others have significant new responsibilities. It appears as though the legislature is serious about the protection of state residents’ personal medical information and identifying demographics.

The purpose of the act: Protection

Expressing concern about the potential for sale or unauthorized disclosure of personal health information, the legislature places tight restrictions on the manner in which patient data may be shared. The legislature notes:

Provisions of recent federal legislation establish incentives designed to increase the adoption of electronic health record systems among certain healthcare providers. The expanded use of such systems is likely to lead to the expansion of the electronic exchange of protected health information, which may require stronger state laws to better ensure the protection of that information. [HB 300] seeks to increase privacy and security protections for protected health information.

In light of the concerns, the legislature mandates authorization before a provider may transfer patient data. HB 300 is intended to provide Texans with significant additional protections beyond those provided by the federal HIPAA privacy rule, and Texas intends to be among the vanguards in health privacy regulation.

The need for protection is obvious. The Ponemon Institute’s December 2011 study—Second Annual Benchmark Study on Patient Privacy and Data Security—estimates that as many as 96 percent of all 72
national healthcare providers surveyed indicated they experienced a data breach in 2011 and that lost and stolen security devices and employee actions accounted for almost half of the breaches.

**The statute’s elements: An overview**

**What is covered? What is PHI?**

The act defines an individual’s protected health information, for a governmental entity, to include any information that reflects that an individual received healthcare from a covered entity that is not public information subject to disclosure by Chapter 552 of the Government Code. For others, the definition of “protected health information” is engrafted from HIPAA.

The act incorporates the HIPAA provisions in effect as of Sept. 1, 2011. The executive commissioner of the Texas Health and Human Safety Commission is to determine whether it is in the best interest of the state to adopt any amendments made to these federal provisions which might be made at the federal level after Sept. 1, 2011. As defined in HIPAA, individually identifiable health information includes demographic data and health information created or received by a healthcare provider, health plan or healthcare clearinghouse that relates to:

- An individual’s past, present or future physical or mental health or condition;
- The provision of healthcare to an individual;
- The past, present or future payment for the provision of healthcare to the individual, and
- The identity of the individual or with respect to which there is a reasonable basis to believe it can be used to identify the individual.

“Individually identifiable” means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient’s name, address, electronic mail address, telephone number or Social Security number or other information that, alone or in combination with other publicly available information, reveals the individual’s identity. Health information means any information, whether oral or recorded in any form or medium, that:

- Is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university or healthcare clearinghouse and
- Relates to the past, present or future physical or mental health or condition of an individual; the provision of healthcare to an individual, or the past, present or future payment for the provision of healthcare to an individual.

HIPAA defines a healthcare provider as “a provider of medical or health services and any other person or organization who furnishes, bills or is paid for healthcare in the normal course of business.” Protected health information, in turn, is defined as individually identifiable health information that is:

- Transmitted by electronic media;
- Maintained in electronic media, or
- Transmitted or maintained in any other form or medium.

Excluded from this definition of protected health information is information within certain educational records and in employment records.

Because the act incorporates the provisions of HIPAA, a more thorough discussion of HIPAA is required for this article. This article will not directly address, however, provisions of related federal laws commonly referred to as HITECH—the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No, 115-5,
123 Stat. 115, Health Information Technology for Economic and Clinical Health (HITECH Act), Sect. 13000, et seq. (Feb. 17, 2009). Detailed analysis of the HITECH provisions and the act are beyond the scope of this overview article. For a discussion of HITECH and the Texas Privacy Laws, see, Patricia Gray’s “Implementing Privacy and Security Standards in Electronic Health Information Exchange” (University of Houston Health Law & Policy Institute, August 2011).

Who is covered? Who is a covered entity?

Section 181 in the Medical Records Privacy statute will continue to define a “covered entity” to be any person who:

- For commercial, financial or professional gain, monetary fees or dues, or on a cooperative, nonprofit or pro bono basis, engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing or transmitting protected health information;
- Comes into possession of protected health information;
- Obtains or stores protected health information under the federal statute and regulations, or
- Is an employee, agent or contractor of one of these persons who creates, receives, obtains, maintains, uses or transmits protected health information.

This includes a business associate, healthcare payer, governmental unit, information or computer management entity, school, health researcher, healthcare facility, clinic, healthcare provider or person who maintains an Internet site. The Texas Medical Records Privacy statute, then, regulates anyone who comes into possession of personal health information (PHI) or is an employee, agent or contractor who creates, receives, obtains, maintains, uses or transmits PHI. There are exemptions in the state act for:

- Workers compensation plans and self-insured workers compensation plans;
- Employee benefits plans;
- Educational records covered by the Family Educational Rights and Privacy Act;
- Nonprofits who pay for indigent medical care but have no medical primary purpose;
- Processors of payment transactions in financial institutions and handlers of criminal offenders with mental impairments. (See Jocelyn Dabeau’s presentation from the “Are Things Really Bigger in Texas?” session at the IAPP Privacy Academy 2011 for more information.)

After the effective date of HB 300, also excluded from coverage of the act will be those involved with crime victim compensation.

What activities are restricted?

Disclosure

It is important to note one key provision of the act. The Texas statute contains one profoundly impactful, although seemingly innocuous, provision. The state statute defines the word “disclose” to mean any action to “release, transfer, provide access to or otherwise divulge information outside the entity holding the information.” It is critical to fully absorb the impact of this definition. Anyone who transfers information, divulges information or provides access to information must be aware of the implications for doing so without an authorization. Taken in its literal meaning, the definition of disclosure is so broad
that it would encompass almost any activity whereby health information or demographics of others is involved. Any information about an individual's condition, care, payment or identity is protected from being divulged or being accessed, no matter the form in which it might be maintained. Any covered entity, including associates of a covered entity, is affected by the statute in some manner. Exceptions are limited and the breadth of the statute's reach is staggering.

Sale of information

Of even greater significance is the act's strict ban on the sale of protected health information. A covered entity may not disclose an individual's protected health information to any other person in exchange for direct or indirect remuneration. Exceptions only allow disclosure to another covered entity under the statute or to a covered entity under the Insurance Code for treatment, payment, healthcare operations and insurance or certain HMO functions or as otherwise authorized or required by law. Further, any charges for the disclosure for treatment, payment, healthcare operations or to perform an insurance function cannot exceed the covered entity's reasonable costs in preparing and transmitting the PHI.

Because the act restricts disclosure of health information for even indirect remuneration, more than an outright ban on the sale of information is restricted. The act restricts any transfer that results in even indirect financial gain that is not associated with treatment, payment, operations, insurance or for compliance authorized by law or required by law. The outright ban on disclosure for even indirect remuneration does not have any mechanism for allowing for disclosure, not even after notice and consent or authorization. Rather, the disclosure for remuneration is flatly banned. Because the act would ban even indirect remuneration, it is possible that the act would implicate, for example, social media interactions or advertising in the form of patient testimonials even if these are the result of patient consent or even the result of patient-initiated activity.

The ability to engage in activities that might result in indirect remuneration with the consent or authorization of the owner of the information and to do so because those actions are protected constitutionally as, for example, free speech or commercial speech, is beyond the scope of this overview article. For discussion of such principles, see, e.g., Sorrell v. IMS Health, Inc., __ U.S. __, 131 S.Ct. 2653 (2011). In Sorrell, the United States Supreme Court determined that restrictions on the sale, disclosure and use of pharmacy records as attempted by implementation of Vermont's Prescription Confidentiality Law, Vt. Stat. Ann., Tit. 18, 4631(d), was unconstitutional because the statute—which imposed content-based and speaker-based burdens on protected expression—banned sales of the information to only some potential users. A complete ban would be more likely to pass constitutional muster.

What additional duties are imposed? Consumer access, notice, training

Patient access to records

The act provides that if a healthcare provider is using an electronic healthcare records system that is capable of fulfilling the request, the healthcare provider, no later than 15 business days following the written request for an electronic healthcare record, must provide the information electronically unless the person making the request agrees to accept the record in another form. An exception is available for records exempt pursuant to 45 C.F.R. § 164.524 for specific types of records such as certain psychotherapy notes, information compiled for use in certain legal proceedings and certain select laboratory records.
The executive commissioner of Texas Health and Human Services, in consultation with the Department of State Health Services, the Texas Medical Board and the Texas Department of Insurance, may recommend a standard electronic format, but any format recommended must be consistent with federal law regarding the release of medical records. As of this writing, the executive commissioner’s office had not yet made a determination concerning the undertaking of this unenviable task. There can be no doubt that the choice of the word “may” in the statute was an intentional one.

Notice and authorization requirements

Any covered entity that creates and receives personal health information must provide notice to individuals if their personal health information is subject to electronic disclosure. The duty to provide notice is, however, only a general one, and the notice can be provided by:

- Posting written notice in the place of business;
- Posting notice on a website, or
- Posting notice in a place where individuals whose PHI is subject to electronic disclosure are likely to see the notice.

According to Texas Health Services Authority General Counsel Jocelyn Dabeau, this notice must be conspicuous and understandable.

Of greatest significance, perhaps, to medical practitioners is the requirement that a covered entity may not electronically disclose an individual’s protected health information to any person without a separate authorization from the individual, or the individual’s legally authorized representative, for each disclosure. The authorization for electronic disclosure is not required, however, if the disclosure is made to another covered entity under the act or to any covered entity as defined by Section 602.001 of the Insurance Code solely for purposes of treatment, payment, healthcare operations, if performing health maintenance organization functions as defined by the Insurance Code or if otherwise authorized or required by state or federal law. The authorization for this disclosure may be made in written form, electronic form or in oral form if the request is documented in writing by the covered entity. The state attorney general will adopt a standard form for use with obtaining authorizations, and the form will also comply with the Health Insurance Portability and Accountability Act and Privacy Standards, if possible. As of this writing, the state attorney general did not yet have an anticipated release date but noted that Section 22 of the act provides for a date of January 1, 2013.

This author assumes that for any such oral authorization to be valid, it would require contemporaneous documentation of the request at the time it was made. As a practical matter, given the audit functions provided in the act (discussed, infra), it would be a best practice to maintain a separate chart for all such patient HIPAA and state privacy law interactions, if possible. In addition, when orally accepting a request for disclosure or accepting a written request in person or electronically, it would be a best practice to again provide general notice about the electronic disclosures.

Training required

Covered entities must provide a training program on state and federal law pertaining to protected health information as it relates to the covered entity’s particular course of business and each employee must be trained but only trained so as to function within their scope of employment. This training must be completed within 60 days of employment and at least once every two years. The covered entity shall require employees who attend training to sign an electronic or written statement verifying attendance at the training program and the covered entity is to maintain the signed statement.
The act, unfortunately, does not indicate that any governmental or educational entity will provide input into the content of any training programs or provide certification for those who will provide the training, however. As of Sept. 15, 2011, no state agency was contemplating oversight of training programs. The State attorney general's office is planning no such function.

The act does not provide a deadline for a covered entity to provide training for those employees who are already employed as of the effective date of the act. However, given the mitigation available as to the potentially onerous penalties for noncompliance—see section below entitled "What are the penalties for noncompliance?"—a covered entity would be engaged in best practices if all employees were provided, at a minimum, training applicable to their job function as soon as practicable.

It can be logically assumed that less substantive training would be required for someone who merely filed a patient’s paper chart onto the proper place on a shelf than would be required for someone who was responsible for the electronic transmission of records or someone who was responsible for the covered entity’s privacy policies or administration. However, anyone who has access to patient records or gains access to patient information is capable of disclosure or breach. In the event that any resulting civil penalty could be mitigated by the existence of a training program (see discussion, infra), providing training to employees and requiring that vendors and business associates, and, particularly, those providing information technology services, also demonstrate compliance with training requirements would be very beneficial. In the event one finds himself or herself with a need, in the future, to argue for mitigation of any civil penalties to be imposed, the existence of evidence of uniform, substantive training will be helpful. In the event training is undertaken from within an organization, best practices would involve retaining records of the training content as well as those who were trained.

What are the penalties for noncompliance? Audits, monetary fines, felony criminal charges, loss of professional licenses

Audits

The Texas Health and Human Services Commission, in connection with the state attorney general, the Texas Health Services Authority and the Texas Department of Insurance, may request that the U.S. secretary of health and human services conduct an audit of a covered entity as to the compliance of the covered entity with HIPAA. The commission is also charged with periodic monitoring and review of the results of audits of covered entities from within the state that are conducted by the U.S. secretary of health and human services. It is unclear what authority the federal auditors would have to monitor for state law violations or whether federal auditors would even be aware of state law violations given that the state law requirements are more extensive than the federal. The U.S. Department of Health and Human Services has embarked on a program of federal audits that is expected to run through December.

If the Texas Health and Human Services Commission becomes aware of egregious violations that demonstrate a pattern and practice, it may require a covered entity to submit to the commission any federal risk analysis that the covered entity prepares in order to comply with HIPAA. In addition, if the covered entity is licensed by a state agency, the commission may request the licensing agency to conduct an audit of the covered entity’s system to determine compliance with the act.

A not insignificant number of potentially overlapping regulatory schemes and enforcement authorities could be implicated by this requirement in the act. For a discussion of the state laws impacting health information regulation, see Cynthia Marietta and Patricia Gray’s "Medical Information Privacy in Texas" (University of Houston Health Law & Policy Institute, February 11) and the section below entitled “Do
other privacy laws exist as well?” The act does not require training for any state or federal agency enforcement personnel.

**Civil penalties for noncompliance**

In addition to the injunctive relief already available pursuant to the current Health and Safety Code Section 181.201(a), the state attorney general may, after the effective date of the act, institute an action for civil penalties for violations of the act not to exceed:

- $5,000 per violation per year if negligent;
- $25,000 per violation per year if knowing or intentional, regardless of the length of time of the violation within the year, or
- $250,000 for each violation if knowing or intentional and for financial gain.

In the event an adjudicator finds that the violations have occurred with a frequency so as to constitute a pattern or practice, the total amount of any civil monetary penalty that the court may assess is not to exceed $1.5 million annually.

A discussion of applicable definitions for the terms “negligence” or “knowing and intentional” is beyond the scope of this overview article. Language contained within the regulations applicable to the Social Security Act seem helpful in describing levels of culpability in civil administrative functions. Penalties may be limited or mitigated, in the event the disclosure was made only to another covered entity for purposes of treatment, payment, healthcare operations or performing functions of a health maintenance organization; if the information disclosed was encrypted or transmitted using encryption technology, or if the covered entity had, at the time of the disclosure, maintained proper procedures including implementation of security procedures and training. Factors are also provided by the act for determining the appropriate financial penalty and include:

- The seriousness of the violation;
- The entity’s compliance history;
- Whether the violation poses a significant risk of financial, reputational or other harm to the individual whose protected health information was involved in the violation;
- Whether the covered entity was working with or as a certified entity, that is, certified to be in compliance with privacy and security standards being developed by the Texas Health Services Authority as per Section 182.108 of the Health and Safety Code for the electronic sharing of protected health information;
- The amount necessary to deter future violations, and
- The covered entity’s efforts to correct the violation.

It is this author’s contention that one should not have to establish harm to the victim in such instances. In order to determine the financial penalty, adjudicators will consider, in the event of disclosure, both monetary and nonmonetary losses.

Nonmonetary losses include humiliation, embarrassment, mental anguish, fear of social ostracism and other severe emotional distress. An excellent discussion of non-economic damages is contained in the Electronic Privacy Information Center’s [FAA v. Cooper, Concerning Emotional Injury as Harm Under the Privacy Act](https://evp.org/medicalinfo/159.html). See also “Will Supreme Court Ruling in Pilot Case Apply to Other ‘Harm’ Cases?” Nonmonetary victim losses also include the increased risk that personal health facts will continue to be
disclosed, the increased risk of identity theft and the increased risk of medical identify theft. Patients themselves express the concern that their data will be misused for commercial gain, that disclosure will result in embarrassment, that disclosure will compromise their personal safety, that their data will be used in a discriminatory fashion impacting their lives and care, that there will be no opportunity to correct any false information circulated and that there will be loss of their data or loss of access to their data. Patients are also concerned about the ability of organizations to accurately provide notification.

Losses to a healthcare provider in the event of an unauthorized disclosure are also not insignificant and include the costs associated with the potential loss of the economic value of a patient who no longer associates with an organization following a breach. At least one study identifies the lifetime economic value, on average, of one patient or customer to fall within a range from $10,000 to more than $1,000,000.

In addition to civil penalties, a covered entity that is licensed by a state agency is subject to investigation and disciplinary proceedings, including probation or suspension by the licensing agency. A license may be revoked if the violations are egregious and constitute a pattern and practice. The attorney general of the state may institute an action for violation of the act against a covered entity that is licensed by a licensing agency of this state for a civil financial penalty only if the licensing agency refers the violation to the attorney general.

What other resources will be available? Websites, standards

Websites

The Texas attorney general is to develop and provide a consumer information website that will include information on the manner in which to make a complaint. As of this writing, the state attorney general did not yet have an anticipated release date but noted that Section 22 of the act provides for a date of May 1, 2013. The author notes that the act becomes effective Sept. 1. Certain materials are directed, by statute, to be included on the website. The Texas attorney general is also charged with monitoring consumer complaints and with reporting on the complaints after de-identifying the protected health information.

Standards

The Texas Health Services Authority is tasked with rulemaking for the certification of entities undertaking the electronic exchange of protected health information. The Texas Health Services Authority is to establish standards for the secure electronic exchange of protected health information. The authority must develop, and submit to the Health and Human Services Commission for ratification, the privacy and security standards for electronic sharing. The authority is also tasked with developing voluntary operations and technical standards for health information exchanges in Texas. Some have expressed concern about the consent options, which will be required in health information exchanges when the act’s requirement is for authorization for the release of information.

What other state statutes are amended or affected? Breach notification laws, the Insurance Code

Breach notification

In HB 300, the legislature also expanded the state’s breach notification requirements already existing in the Business and Commerce Code at Sections 521.053 and 521.151. The expanded notification will require
notice not only to state residents in the event of a breach, as previously required, but also to all affected individuals. Because notice is to be given to all individuals and not only state citizens, the reach of the statute in its regulation of any covered entity within the state will undoubtedly have nationwide or even global impact. The Dallas Regional Chamber of Commerce estimates the healthcare industry contributes $52 billion dollars annually to the Dallas-Fort Worth area alone, supporting an estimated 601,000 regional jobs and driving up to 15 percent of the area economy. In addition to time and productivity losses in the event of a breach, the economic impacts identified in one study estimated costs for data breach incidents to hospitals surveyed to be in a range from $10,000 to more than $10,000,000 per entity in a two-year period.

Texas's Business Code already includes notice requirements for breaches of information pertaining to “personal identifying information,” identified in the Business Code breach notification provisions to include biometric data, the physical or mental health or condition of an individual, the provision of healthcare to an individual or the payment for the provision of healthcare to the individual. HB 300 added to the breach notification penalty provisions of Business and Commerce Code Section 521.151 the ability to recover additional civil penalties of up to $100 per day, per individual affected, for an unreasonable delay in notification or failed notification of a breach of data. Although the breach statute does not incorporate the act’s definition of PHI, the definition employed in the Business Code breach statute is broad enough to include PHI. Including enhanced fines for the failure to notify in the event of a breach within the act without revising the Business Code to include a revised definition of PHI demonstrates the legislature’s intent for the two statutes to work in an interrelated fashion.

Offenses for the use of a scanning device or re-encoder to access, read, scan, store or transfer information encoded on the magnetic strip of a payment card without the consent of an authorized user of the payment card and with intent to harm or defraud another were previously codified as a Class B misdemeanor under the Business and Commerce Code. Now, however, if such an offense also involves protected health information as defined by HIPAA, the offense is defined as a felony. If an element of the crime was committed prior to Sept. 1, 2012, the offense was committed prior to the effective date of the act. It is worth noting again that payment processors at financial institutions are not covered entities, however.

The Insurance Code

The State Insurance Code, Chapter 602, was amended by HB 300 to require those covered by Chapter 602 of the Insurance Code to comply with Chapter 181, the Medical Records Privacy statutory provisions. Consequently, the act now also pertains to insurance companies that are exempt from HIPAA, including:

- County mutual insurance companies
- Farm mutual insurance companies
- Fraternal benefit societies
- Group hospital service corporations
- Lloyd's plans
- Local mutual aid associations
- Mutual insurance companies
- Reciprocal or inter-insurance exchanges
- Statewide mutual assessment companies
- Stipulated premium companies
- Health maintenance organizations
Insurance agents

These individuals and organizations must comply with act’s provisions when it becomes effective on Sept. 1. The distinctions in the Insurance Code between “health information” and “nonpublic health information,” defined by Section 602.001 of the Insurance Code, is beyond the scope of this overview article. Section 602.002 of the Insurance Code provides that this chapter of the insurance code does not apply to a covered entity that is required to comply with the standards governing the privacy of individually identifiable health information adopted by the United States Secretary of Health and Human Services under Section 262(a), Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d, et seq.). Section 602.003 of the Insurance Code indicates the chapter does not preempt or supersede state law in effect on July 1, 2002, that relates to the privacy of medical records, health information or insurance information. Section 602.053 of the Insurance Code provides exceptions that allow a covered entity to disclose nonpublic personal health information to the extent that the disclosure is necessary to perform the specified insurance or health maintenance organization functions, as identified in that provision, on behalf of the covered entity. The definition of “health information” in the Insurance Code does not include age and gender.

Do other privacy laws exist as well?

Other state statutes and common law principles are not implicated by the act and are not subsumed by the act’s provisions, including the existing body of legal and ethical principles pertaining to patient privileges. There are myriad additional privacy statutes and regulations that will not be subsumed within the act. There are other state statutes that contain restrictions on the disclosure of records currently applicable to a variety of healthcare facilities, such as nursing facilities, rehabilitation facilities, surgery centers and emergency rooms. Mental health professionals also have their own patient privilege laws and ethical codes, particularly as to psychotherapy notes from a patient whose provider determines his best interests would not be served by disclosure. HIV and AIDS records and records pertaining to other communicable diseases are also subject to their own distinct disclosure provisions. Genetic information is separately regulated, as are substance abuse records, certain health study records, occupational condition reporting and records pertaining to minors, inmates and students. Biometric identifiers, Medicaid, State Children’s Health Insurance Program Beneficiaries, other government records containing health information and peer review committee investigation records are all given separate treatment in Texas law. Some of these laws, unlike the act, provide individuals with a cause of action for unauthorized disclosure.

It is clear that attorney-client privileges would apply as to disclosures between an attorney and the attorney’s own client. It seems far less clear that attorneys would not be considered a covered entity when handling the protected health information of others in other instances. The legislature clearly carved such exceptions where it thought them to be applicable and the legal profession was not provided with an exception.

Conclusion

HB 300 act is aggressive in its reach. Its penalty provisions, if and when enforced, will almost certainly be a solid deterrent to all except the most unscrupulous and most careless. It is unfortunate that the burdens of compliance could further exacerbate the already burdensome administrative overlay existing for those in the state who provide healthcare and related services. Given the enormity of the need for the protection of health information and patient demographics, however, state governments can do no less than take an aggressive approach to supplement federal law pertaining to medical privacy. The
provisions of House Bill 300 could create enormous exposure to covered entities as well as licensed individuals and groups. It should follow, then, that associations and individuals will be highly motivated to comply with the act and to protect personal health information. The legislature was clearly serious, and the citizens of the state now wait to see whether enforcement will bear out legislative intent.


B. Joyce Yeager is a licensed attorney and Certified Information Privacy Professional. She prepared this article while practicing law in Texas. Yeager is now an assistant attorney general for the Office of the Attorney General of Missouri. She is also the founder of Amenable Though, LLC, an organization committed to education and the arts. She can be reached at b.joyce.yeager@gmail.com. A fully annotated version of this article is available from the author.
Experts question whether the EC’s “Right To Be Forgotten” has forgotten a few key points

By Angelique Carson, CIPP/US

Within the European Commission’s draft data protection framework is a provision for “the right to be forgotten and to erasure.” The provision’s concept isn’t entirely new to member states. Article 12 within the 1995 Data Protection Directive allows for the right to erasure. But where Article 12 grants data subjects rights to request that data controllers correct or erase data concerning them and to lodge a complaint to the supervisory authority, among others, the new proposal would allow data subjects to ask the data controller to delete their data and cease disseminating, even if consent was at one time given. The data controller would then also be responsible for taking all reasonable steps to alert third parties of a data subject’s request to correct or erase the data.

Tanguy Van Overstraeten, Partner at Linklaters in Brussels, said the right to be forgotten has been proposed to reinforce existing rights because there was a perception that these rights weren’t sufficient.

“The aim was not to significantly change the reality on the ground but the way the proposed provisions are drafted may have completely unintended and adverse consequences,” Van Overstraeten says.

Others say the provision will have major repercussions. George Washington Law Professor and legal commentator Jeff Rosen wrote for Stanford Law Review, for example, that despite European Commission Vice President Viviane Reding’s assertion that the right is a “modest expansion of existing data privacy rights,” in fact, “it represents the biggest threat to free speech on the Internet in the coming decade.”

Stakeholders have expressed particular concern with the proposal’s assertion that search engines and social media networks are defined in the draft as data controllers of the content users post and store on their sites.

Facebook UK Public Policy Director Simon Milner has said the proposal is troubling because “It is a right that someone can delete what they have posted but should not be able to delete what someone has posted about you.”

Vint Cerf, one of the co-founders of the Internet, has condemned the right to be forgotten provision, citing its impracticality. “It’s very, very hard to get the Internet to forget things that you don’t want it to remember because it’s easy to download and copy and re-upload files again later,” Cerf told The Daily Telegraph.

Van Overstraeten said the provision should at least draw a line between user-generated content—information a user voluntarily posts to a website, for example—and information posted by a third party.

User-generated content “should in principle be under your control. As a result, you may be entitled, to the extent of course it is still feasible, to have that information deleted if you decide at some point in time it is no longer suitable,” Van Overstraeten said. “On the other hand, the information that comes from third parties like information containing personal data posted by a journalist should remain subject to other individual rights such as the right of reply. In my opinion, there is no way the right to be forgotten could be exercised in that context.”
Spanish attorney Cecilia Alvarez Rigaudias of Uría Menéndez agreed.

“You may have other content posted by your family, friends or others, which at the end of the day may cause harm to you. This could also be the newspaper or media where the freedom of expression and freedom of speech, as fundamental freedoms, must be balanced vis-à-vis privacy,” she said. “There also could be situations where the legislation obliges to publish certain information like in judicial rulings, or information which is published in the official gazette in order to provide relevant information to the market, and therefore it’s difficult to assess whether you really have a “right to be forgotten” just because you do not want this to be available.”

Françoise Gilbert of IT Law Group adds that in the U.S., companies are "scratching their heads and saying, ‘How are we going to do this? We don’t think this is feasible at the very basic technical level.’"

Most troubling to her clients is the provision’s requirements that in the case of an individual’s request to remove data concerning him or her, “the entity not only has to remove the information but also has to contact third parties and tell them to remove the information. It’s very difficult to implement,” Gilbert said. “Only removing someone’s information can be difficult because, in one context, the information can be in many places. On top of that, you have to contact third parties.”

Ahead of the draft provision, courts in several jurisdictions have heard arguments based on varying interpretations of the right to be forgotten. In March, the UK government called for legislation that would force Internet companies to “proactively filter search results and require court-ordered material to be suppressed,” Deutsche Welle reported. In the same month, a Tokyo District Court approved a petition to require Google to delete terms from its auto-complete search feature after a man alleged the feature resulted in the loss of his employment. Earlier this year, the BBC unveiled a digital charter that will allow users of its web services to have all of their data deleted, and Spain’s government ordered Google to halt indexing of data on certain individuals after 90 complaints to Spain’s Data Protection Agency, a move Google said would have a “profound chilling effect on free expression without protecting people’s privacy,” according to The New York Times.

Also in March, a “right to be forgotten” case was dismissed by a Spanish court. A company argued online images harmed its reputation, but the court ruled that Google Spain “lacked standing to be sued” because it is a subsidiary.

Search engines are especially concerned with their level of responsibility under the draft proposal, according to Rigaudias.

“With respect to the fact that they don’t want to create precedent, they do not want to be held liable as intermediaries of information society services regarding contents that they have not created. I think they could be more worried and concerned about this specific issue than the data protection questions that are under discussion.”

Rigaudias said her clients feel “there is an overreaction with respect to the right to be forgotten, because the right to obtain a certain cancellation of data already exists in the data protection regulation since 1992.”

In a blog post, Google Chief Privacy Counsel Peter Fleischer wrote that because the Internet’s vitality shows no signs of slowing down, it is “vitally important that both those who provide online services and those who use them have a clear understanding of how a concept such as the right to be forgotten might apply.”

Fleischer noted there are practical and technical barriers to hosting platforms’ ability to comply with some of the proposal’s provisions, including the timeframe in which a platform must comply with a user’s
request for data deletion and the expectation that a platform will ensure third-party compliance with data deletion. However, in the end, he said Google is “supportive of the principles behind the right to be forgotten” and believes “it’s possible to implement this concept in a way that not only enhances privacy online but also fosters free expression for all.”

Rosen told The Privacy Advisor freedom of expression is exactly what’s at stake.

“I think the proposal is so broadly drafted that it could require search engines to remove a lot of speech that they currently assume is protected on the net, and uncertainty about whether they could be liable up to one percent of their income might well lead them to remove even more speech that the proposal requires,” Rosen said.

Additionally, Rosen said the companies concerned aren’t staffed to make judgment calls on what material should be taken down upon a user’s request and which is exempted from the law because it falls under the right to “freedom of expression” or for reasons of “public interest in the area of public health” or for “historical, statistical and scientific research purposes,” as the proposal provides.

“Right now, the first responders at Google and Facebook who will decide whether or not to take down the request tend to be 17-year-olds in flip flops in Silicon Valley—not people who have the resources or training to be making these case-by-case decisions,” Rosen said.

Meanwhile, Rigaudias said third-party posts should be taken into consideration.

Gilbert wants to see clarifications from the EC on what the provision aims to achieve at its core.

“I see a pretty significant disconnect between the speeches that Ms. Reding has made or representatives of the European Commission have made about what this proposal is supposed to be doing and what the text of the actual proposal says,” Gilbert said.

Experts seem to agree that the current proposal needs some tweaking before it’s ready for the books.

“From a legal perspective, there is a need to revisit these clauses to make them more technically practicable in a complex digital environment, to specify their exact scope of application and make sure they are aligned with other fundamental or individual rights. I think some clarifications could be taken from recent speeches of Vice-President Reding and included in the draft which definitely needs additional specifications to make compliance with the rule more attainable in practice” said Van Overstraeten. “Businesses need certainty,” he added.

“The proposal needs to be revised,” Rosen said. “I’m frankly surprised that in the face of vigorous criticisms, Viviane Reding has not narrowed the proposal to what she originally suggested, and I hope that she will. There are certainly lots of people who are concerned about this.”
Online piracy eradication efforts spark privacy concerns

Protests against the alphabet soup of competing anti-piracy and cybersecurity information-sharing bills—ACTA, CISPA, PIPA, SOPA—highlight the difficulty of balancing intellectual property protection and Internet freedom

By Mathew J. Schwartz

Must preventing online piracy and product counterfeiting, and stopping Internet-borne attacks, come at the expense of safeguarding people’s privacy?

Recently introduced proposals—ACTA, CISPA, PIPA, SOPA and more—in Europe and North America have offered solutions to the problems of intellectual property theft and nonstop attacks against business networks. But the sheer scale of popular protests against many of these legislative proposals suggests that balancing intellectual property rights and civil liberties won’t be easy.

Here’s a look at some of those legislative trends and why they’ve so often triggered privacy concerns.

Sharing cybersecurity intelligence (CISPA, CSA)

The stated goal of the House Cyber Intelligence Sharing and Protection Act (CISPA) is to enable U.S. intelligence agencies to share attack signatures with private businesses to help them better spot and block the seemingly unending stream of malware, phishing campaigns and advanced persistent threats now targeting their networks and too often breaking in.

While sharing attack data sounds fine in theory, CISPA has raised fears that private businesses might share any data they collected—including employees' browsing habits and communications—with the Department of Homeland Security (DHS), which could then share it with the National Security Agency. Furthermore, assuming that the attack-signature data is better than what businesses currently have access to, any business that receives the data wouldn’t be held legally accountable for using it.

Despite that criticism, CISPA was passed by the House last month and has moved to the Senate, where Sen. Joe Lieberman (I-CT) has introduced the Senate’s version, dubbed the Cybersecurity Sharing Act (CSA) of 2012. But the new bill is already facing CISPA-like criticism.

"I have serious concerns about this bill," says Sen. Al Franken (D-MN) via e-mail. "As written, the legislation moves aside decades of privacy laws to allow companies to freely monitor American citizens’ communications and give their personal information to the federal government—and grants companies near total immunity for doing so."

Surveillance modernization (CCDP, C-30, H.R. 1981)

While critics of CISPA and CSA say they will result in excessive surveillance of innocent people, many countries are pursuing “surveillance modernization” bills designed for that express purpose. Recently, for example, Britain’s coalition government began floating the Communications Capabilities Development
Program (CCDP), which would allow UK intelligence agencies to keep the e-mail and other communications records of everyone in the country for up to 12 months.

Likewise in Canada, Public Safety Minister Vic Toews has been pushing a controversial online surveillance bill known as C-30, purportedly to combat child pornography. As currently drafted, the bill says that under “exceptional circumstances...any police officer” could obtain information about a subscriber from a telecommunications provider. But critics have noted that while the bill’s title says it’s meant to combat child pornography, nothing in the bill’s text says how that will happen. Similar legislation in the United States, HR 1981, would require service providers to retain a log of subscriber-related information, including credit card data, for at least 12 months.

But such mass surveillance could reshape current approaches to law enforcement. “That makes us all a suspect,” says Jim Killock, executive director of the Open Rights Group. “Instead of being under surveillance when there is evidence of wrongdoing, you will be under suspicion by default.”

Furthermore, storing all of that information in one place would likely create entirely new security risks. “These databases would also be a new and valuable target for black hat hackers, be they criminals trying to steal identities or foreign governments trying to unmask anonymous dissidents,” according to the Electronic Frontier Foundation.

Blocking rogue websites (SOPA, PIPA)

Moving into the anti-piracy realm, the purpose of the U.S. House bill titled “Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act” (Protect IP Act, or PIPA), in the words of chief sponsor Rep. Lamar Smith (R-TX), was “to enact legislation that protects consumers, businesses and jobs from foreign thieves who steal America's intellectual property.” The Stop Online Piracy Act (SOPA), authored by Sen. Patrick Leahy (D-VT), pursued a similar goal.

The bills, introduced in 2011, would have required service providers to use DNS filtering to forcibly reroute consumers from sites deemed to be violating U.S. copyright law. They also promised legal protections for payment processors who declined to send money to organizations that the U.S. government accused of violating copyrights, whether that involved digital media, counterfeit clothing or generic pharmaceuticals.

A number of leading technology voices, however, branded the proposed legislation as censorship, as well as being unworkable and likely costly. “There is ample evidence to suggest that DNS filtering will not be effective against infringement. There are just too many ways for determined seekers and purveyors to get around the blocks,” according to Center for Democracy and Technology (CDT) policy analyst Andrew McDiarmid.

To protest SOPA and PIPA, thousands of websites—including Wikipedia—“went dark” for a day. Meanwhile, the White House threatened a veto.

Soon after, both bills were shelved. But a proposal from Rep. Darrell Issa (R-CA) and Sen. Ron Wyden (D-OR), the bipartisan OPEN Act, pointedly avoids DNS filtering, and could be a way forward. According to the bill’s sponsors, who’ve launched a website aimed at crowd-sourcing improvements to the bill, it’s designed to address two principles: “First, Americans have a right to benefit from what they’ve created. And second, Americans have a right to an open Internet. Our duty is to protect these rights.” While the
EFF called the bill “far from perfect,” it did laud the lawmakers for pursuing “an open process befitting an open Internet” in their drafting of the bill.

**IP agreements stoke unrest (ACTA)**

Like SOPA and PIPA, the Anti-Counterfeiting Trade Agreement (ACTA) is designed to protect intellectual property rights, including targeting the sale of counterfeit goods and generic medicines. ACTA differs, however, in that it's an international agreement— provisionally signed by more than 20 EU member states as well as the U.S., Australia, Canada, Japan and other countries.

But ACTA critics worry that the international agreement could lead to Internet censorship, and those fears have triggered protests in Europe that far exceed the scale of U.S. resistance to SOPA and PIPA.

“With ACTA, you saw in Berlin the largest demonstrations on a transatlantic issue since the Iraq war— almost 100,000 people,” Tyson Barker, a fellow at the Truman National Security Project, told The Privacy Advisor. "Poland was the same, as was the Czech Republic. It’s no coincidence that these are the same states that have known dictatorships and the extremes of domestic surveillance.”

In other words, ACTA is far from a done deal.

**Facing common problems but still seeking solutions**

Furthermore, the business and surveillance initiatives may now be heading for a transatlantic showdown.

“The debate over privacy, data protection, e-commerce, cybersecurity, and IPR (intellectual property rights) online is going to be a huge fault line between the United States and Europe, and until they get on the same page, they will be vulnerable to divisions by rising players like China and India,” Barker said.

Of course, assuming that North America and Europe can reach an agreement on ACTA first assumes that EU states can reach their own agreement.

“It’s like the narcissism of petty differences, but these stances are so culturally embedded that they’re going to be difficult to dislodge or change,” Barker said.

Mathew Schwartz reports on information security and privacy issues for InformationWeek, The Privacy Advisor and Inside 1 to 1: Privacy.

Read more by Mathew Schwartz:
- Social networks seek workplace privacy protections
- Facing the privacy implications of IPv6
- How 9/11 changed privacy
- Privacy software to protect patient records
Privacy considerations for successful navigation into the federal cloud space

By William C. Hoffman, Jr., CIPP/G, CIPP/US

As the nation’s first federal chief information officer (CIO), Vivek Kundra published a “25 Point Implementation Plan To Reform Information Technology Management.” This plan’s overarching goal was to deliver more value to the American public with regard to IT spending. In addition, he put in place a “Cloud First” policy. This was done to better serve the American people by:

- Accelerating a safe and secure adoption of cloud computing;
- Shifting up to $20 billion worth of federal IT spending to cloud-based solutions, and
- Focusing on mission-critical tasks instead of on purchasing, configuring and maintaining redundant infrastructure.

All federal agencies are in the process of moving to the cloud. My question is: How do we continue to facilitate this transfer of data, and consolidation of redundant infrastructure, while at the same time ensuring security and privacy protections are in place to foster the trust of the American people? Our entire democracy is built upon trust.

All federal agencies must have a cohesive strategy in order to protect the data that has been entrusted to them, regardless of where the data is actually stored. Federal managers must have an understanding of the level of risk associated with their specific cloud strategies.

Privacy must be built into the front end of the overall process and not added on towards the end. This will require an immense shift in the mindset of all participants of the team. This is an enormous cultural change that will require cross-organizational training to all members of the system design life cycle (SDLC) as well as all acquisition pipelines.

Any consideration to place federal data into the cloud environment cannot truly be successful without the cooperation and thorough integration of the cloud-based solution through your security, privacy, acquisition, contracts, management and legal counsel’s offices. Ten specific areas are highlighted in the paper titled, “Creating Effective Cloud Computing Contracts for the Federal Government, Best Practices for Acquiring IT as a Service.” The 10 areas are:

- Selecting a cloud service
- Cloud Service Provider (CSP) and End-User Agreements
- Service Level Agreements (SLAs)
- CSP, agency and integrator roles and responsibilities
- Standards
- Security
- Privacy
- E-Discovery
- Freedom of Information Act (FOIA)
• E-Records

The Feb. 24 document is a first step in providing guidance to successful implementation of the “Cloud First” strategy. In addition to the 10 areas mentioned, the document also has an Appendix A, where suggested procurement preparation items are listed in checklist-formatted questions in the areas of general questions, service-level agreement, CSP and end-user agreements, e-discovery, cybersecurity, privacy, FOIA and recordkeeping.

These questions will help in the preparation of a successful launch of IT services into the cloud.

Listed below are general ideas that will assist you in your attempt to protect the data:

• Agencies should ensure the CSPs have completed a Security and Privacy Authorization to assess the risk level and to have it at a level commensurate with the sensitivity level of the data to be stored into the cloud.
• Contracts with CSPs shall be prepared with great effort and in concert to include all stakeholders and experienced members of the team—security, privacy, acquisitions, contracts and management—to ensure that specific items are included in the contract. Failure to put forth sufficient effort in this stage will greatly limit your recourse in the event of a loss incident and put your agency at risk of unsecured data being lost or stolen. This will result in having to incur penalties, and fines associated with the loss, not to mention the embarrassment as an agency to the general public.
• All federal agencies are required to use the Federal Risk and Authorization Management Program (Fed RAMP). This is a platform set up in December of 2011 by the White House to help federal agencies with security risks and computing costs. Fully understanding the security risk to the data will allow for preparing controls and protection methodology to be incorporated into the cloud solution.

Current Federal CIO Steve VanRoekel is in place to help build an IT infrastructure that works better for the American people. Maximizing IT return-on-investment and improving the productivity of all IT systems is essential in order to obtain the desired positive effect as we move forward.

In February, the Obama administration held a privacy summit at the White House that produced a “Consumer Privacy Bill of Rights.” This is supposed to be a blueprint to give users more control over how their personal information is used over the Internet and help businesses maintain trust in the rapidly changing digital environment. Elevating privacy to the point of a White House visit by privacy professionals clearly shows the importance of privacy matters to the federal government. It is our job as privacy professionals to leverage off of this historic first step and continue to protect the privacy of information as we collect it in our daily work. Throughout all of this innovation, IT sharing, consolidation and cost savings-efforts, one thing must remain constant. Regardless of whether your information is being collected by commercial entities, or by the government, one best practice statement soars above all others: “If you collect it, you must protect it.”

William Hoffman, CIPP/G, CIPP/US, senior privacy consultant, is a retired naval security officer providing privacy expertise to government agencies and currently sits on the IAPP Publications Advisory Board. He recently conducted a privacy workshop entitled “Navigating the Federal Maze: Federal Legislation and the Privacy Impact Assessment Process” at the IAPP Privacy Academy in Dallas, TX.
Check: Are you ready for social media?

By Lothar Determann and Arlan Gates

Social media brings opportunities and risks. Companies have to prepare and position themselves. This article summarizes a few key considerations from different angles for a checkup on your company’s social media readiness.

Are you using the social media platforms you need and for appropriate purposes?

Open, public platforms come with a critical mass of users, content and functionality. If your competitors are already there, you may have to follow. If not, you may want to be first. Or, perhaps you may rule a platform out. If you adopt an open platform, you need to decide what purposes you allow employees to use it for; e.g., marketing, information gathering, communicating with certain communities. With respect to the intended use, the platform’s data processing practices must be compatible with your company’s privacy compliance program and contractual commitments to your customers and employees.

On closed, proprietary platforms, confidentiality and data security can be as strong as with respect to other outsourced information technology services; e.g., corporate e-mail. You need to vet the platform vendor like any other data processing services provider with respect to data security. If the vendor meets your data security requirements, you may theoretically be able to use such platforms for most or all types of company communications. Closed tools tend to be useful, however, only for some forms of company-internal cooperation. The very fact that they are closed limits their usefulness in many other respects and renders them unsuitable for certain usage types; e.g., advertising, product placement, etc. Thus, closed platforms are often not an alternative to open platforms.

Consider a mix of open and closed social media platforms for different purposes. Some companies additionally create customized platforms or at least customized applications or features for existing platforms. Then, establish clear rules and guidance on how your employees should and must not use particular social media platforms.

Do you own what you think you own?

To protect your company’s intellectual property, review the platform providers’ services terms and technical realities carefully in advance. Confirm whether your company can own an account—or only individuals—and whether a leaving employee can, and can be compelled to, transfer accounts, connections, data, content and other intangibles upon termination of employment. You may also want to reach an explicit understanding and agreement with your employees regarding what will happen to social media accounts when employees leave.
Is your data privacy compliance program ready for social media?

Privacy on social media is a hotly debated and widely misunderstood concept. Providers have to disclose—and in some jurisdictions obtain consent regarding—their data processing practices for marketing purposes. But, the brunt of responsibility, risks and compliance obligations is on the users of social media platforms who upload information; i.e., you and I and our companies (Determann, “Social Media Privacy—12 Myths and Facts,” Stanford Technology Law Journal, forthcoming 2012). Companies that let their employees use social media should check whether processes and documentation supporting the company’s data privacy law compliance program need an upgrade in the social media age. Privacy statements, employee notices, customer consent forms, acceptable use policies, monitoring protocols, anti-spam law compliance mechanisms—many processes and policies have been designed with particular technologies, communication patterns and user behavior in mind and will need different wording and examples to appropriately capture social media platforms. Providers of standard or customized proprietary social media platforms may have to be asked to sign up to the EU Standard Contractual Clauses, Safe Harbor Onward Transfer Agreements or similar form contracts required by companies’ compliance programs. Companies have to conduct some level of due diligence on all service providers’ data processing and security practices, including social media platforms used by employees.

Are your employee policies up to date with respect to social media?

Employees need to be informed about your answer to the threshold question whether your company prescribes, prohibits or permits social media usage and which platforms to use for work-related purposes (Determann, “Social Media @ Work—Legal and Business Considerations for Global Companies,” BNA Data Privacy & Security Report and World Data Protection Report).

Policies about monitoring employees, networks and computers may have to be updated to specifically state if and how the employer monitors employees using social media. This is necessary to prevent U.S. employees from developing limited expectations of privacy, which could then restrict the employer’s ability to monitor and protect data security, trade secrets and compliance more generally. With respect to employees outside the United States, however, employers have to respect limitations under data protection and communications laws abroad (Determann/Sprague, “Intrusive Monitoring: Employment Privacy Expectations Are Reasonable in Europe, Destroyed in the United States,” Berkeley Technology Law Journal).

With respect to social media that companies encourage or require employees to use, employees should be informed that providing pictures and populating certain data fields is voluntary and potentially not recommended; e.g., due to concerns regarding possible age or racial discrimination.

Employees must protect trade secrets and personal data—on social media as much as elsewhere. With respect to social media, companies find a greater risk that through connections with company-internal and external persons and informal communications modes, employees tend to disclose information more lightly. Thus, reminders may be in order regarding what particular social media platforms may and must not be used for (Determann/Krüdewagen, “Policing Social Media Policies,” The Recorder).

Employees should generally not be allowed to anonymously endorse their company’s own products or criticize competitors.

If employees are permitted or expected to comment publicly on company affairs; e.g., financial results, product defects, litigation, with disclosure of the company affiliation, employees traditionally have to undergo certain controls and legal review. Such requirements should be applied regardless of the
publication forum. Ad hoc publicity on social media platforms can expose a company to liability as much as a formal filing with the SEC and should therefore be pre-reviewed just as carefully.

Companies need a process to prevent value associated with social media accounts to leave the company with employees who quit or are fired. Company-owned accounts should be transferred from departing employees as part of the exit interview. With respect to employee-owned accounts, the employer may be entitled to copies of some or all data in the account if adequate agreements with the employees are put in place, ideally in the new hire process.

Litigation holds and rules on communications with witnesses, defendants and jury members apply to communications and information on social media platforms as elsewhere. Company policies and employee notices may have to be updated to remind everyone involved.

If a company decides to issue a separate social media policy, it should include a reminder that employees are obligated to comply with laws and company policies also in the social media context, including rules against harassment, distribution of obscene or illegal content, defamation, etc.

**Does your HR group know what to do?**

Social media platforms provide a rich source of information that companies are interested in for purposes of selecting job candidates or investigating employee misconduct. But, companies should limit the information intake—or separate research staff and HR staff—to prevent setting themselves up for discrimination charges. Demanding social media account passwords from employees or candidates is also hardly advisable; it is in conflict with platform provider terms, with possible implications under the Computer Fraud and Abuse Act, and is about to be prohibited in a number of U.S. states.

If companies want to collect information from social media platforms or include information regarding social media presentations of candidates or employees in files or human resources information systems, they may be obligated to notify the candidates or employees under data protection laws in Europe and many other jurisdictions.

**Is your IT department on top of new social media technologies?**

Information technology and security personnel should help develop guidance on how to deal with social media; e.g., how to protect the company and its employees from new security threats and how to vet safe apps that employees are allowed to download to company devices. Also, new processes and technological solutions may be necessary with respect to employee monitoring, investigations and erasing data from retired devices.

**Are sales and marketing under control?**

Anti-spam laws apply also on social media platforms (Determann/Gates, "Rethinking Compliance Strategies: After EU, U.S., Other Countries, Canada Passes Anti-Spam Law," *BNA Data Privacy & Security Report*). Often, the platform operators impose additional restrictions on direct marketing. Marketing personnel has to be trained on applicable restrictions and practical compliance options—where available. On some social media platforms, it is impractical to scrub against opt-out lists or include unsubscribe verbiage in posts. Such platforms should probably not be used for direct marketing. Also of concern are European restrictions on cookies and social media plug-ins; information gathering practices involving "scraping" of social media sites contrary to the sites’ terms; manipulating competitors’ Wikipedia pages; promoting or administering contests or sweepstakes; ads directed at children; endorsements, reviews or testimonials without disclosure of company affiliation or financial connection, and anonymous product reviews by employees.
Have you considered industry-specific, regulatory requirements?

Compliance officers and in-house lawyers should determine what additional steps they should take to extend the company’s overall compliance program to cover social media-related risks. For example, companies in the pharma and healthcare sector should implement processes to ensure that they adequately address reports on adverse events relating to medicines or treatments, as well as promotion of off-label use that they may receive through social media channels.

Are you regulating too much?

In the United States and many other jurisdictions, employers must respect the right of employees to engage in concerted action; e.g., discuss working conditions with co-workers. In many European jurisdictions, companies may have to consult with works councils or trade unions if they want to monitor employee conduct and performance via research on social media. Employees can assert rights under constitutional principles, which apply directly or indirectly in many countries and can protect an employee’s freedom to complain about working conditions or co-workers. Companies should periodically review their social media policies and communications to ensure that they are not violating laws protecting workers’ rights.

Are you training enough?

Technologies, communication patterns and social conventions develop rapidly and chaotically on new media. Most abuses and problems relating to social media platforms should not be blamed on the platform operators and do not result from employee mischief but rather by accident or due to lack of sophistication. Even more important than regulation is, therefore, ongoing training on how employees can and should use social media, in hands-on workshops, with information on how the platforms and technologies work, case studies on mishaps and “teachable moments,” role modeling, simulating real-life situations and special coaching for company spokespersons.

Do you know the latest and coolest social media application?

We finalized this checklist in mid-May. When IAPP publishes it, it will be outdated. Once a month, it will be time to add new points to social media checklists. So, check with your kids and friends what the latest and coolest social media application is and how you can best use it.

Prof. Lothar Determann practices data privacy and technology law as a partner in Baker & McKenzie’s Palo Alto office, and teaches data privacy, e-commerce and computer law at University of California, Berkeley School of Law (Boalt Hall), Hastings College of Law, Stanford Law School and Freie Universität Berlin. He may be reached at Lothar.Determann@bakermckenzie.com.

Arlan Gates practices marketing and technology law as a partner in Baker & McKenzie’s Toronto office. He may be reached at Arlan.Gates@bakermckenzie.com.

Read more by Lothar Determann:

Data privacy in the cloud—A dozen myths and facts
New data privacy law in Mexico
New European Standard Contractual Clauses for data processors
Employee monitoring technologies and data privacy - no one-size-fits-all globally
Will Supreme Court Ruling In Pilot Case Apply to Other “Harm” Cases?

By Angelique Carson, CIPP/US

Plaintiffs are increasingly filing privacy lawsuits that allege harm and seek compensation. But to date, courts have grappled with discrepancies between plaintiffs’ “harm” claims and the scope of the law—particularly when the harm can't be qualified, such as in cases of emotional distress or humiliation, leaving many plaintiffs empty-handed when the judge strikes the gavel.

Experts say the recent Supreme Court ruling in Federal Aviation Administration (FAA) v. Cooper illustrates the difficulty plaintiffs face in collecting damages under the Privacy Act of 1974, which dictates how agencies under the Executive Branch manage confidential records.

In the case, pilot Stan Cooper withheld his HIV status from the FAA in applying for the certificate he needed to comply with FAA medical standards on four separate occasions. When his health deteriorated in 1995, Cooper applied to the Social Security Administration (SSA) for disability—revealing his HIV status. A cross-agency investigation compared FAA and SSA records and found Cooper had lied. Following a guilty plea, Cooper’s pilot certificate was revoked and he was sentenced to two years of probation and a $1,000 fine for intentionally withholding information from a government agency.

In turn, Cooper sued the FAA, its parent, the Department of Transportation and the Social Security Administration for violating the Privacy Act by sharing his medical records among themselves; revealing his HIV diagnosis, and thus causing him “humiliation, embarrassment, mental anguish, fear of social ostracism and other severe emotional distress,” the suit alleged.

The Ninth Circuit Court of Appeals in San Francisco ruled in February 2010 that Cooper could seek damages for emotional distress, as the San Francisco Chronicle reported. But the U.S. Supreme Court voted 5-3 in March of this year that though the government had violated the Privacy Act, Cooper could not collect damages for the emotional distress he suffered because “the act does not authorize the recovery of damages from the government for nonpecuniary mental or emotional harm.”

Since then, the Electronic Privacy Information Center has proposed changes to the Privacy Act that would in fact compensate individuals for nonpecuniary harms such as mental or emotional distress. Sen. Daniel Akaka (D-HI) introduced a bill in October 2011 that would revise the Privacy Act to allow for civil and criminal penalties for Privacy Act violations.

D. Reed Freeman, CIPP/US, of Morrison Foerster, said courts are increasingly hearing class-action cases that seek “harm” damages and that to date, defendants have largely been successful in having the allegations dismissed, citing plaintiffs’ failure to meet the Constitution’s “cognizable harm” statute.

“What you’re seeing is that by and large, plaintiffs have a very difficult time proving harm in the data loss or theft cases,” said Andrew Serwin of Foley & Lardner. Serwin added that although sovereign immunity applies in the Cooper case, “even now in the public-sector side, you’re seeing courts say ‘you can’t prove damages, and therefore, you can’t state a claim.’”

However, FAA v. Cooper, while illustrative of the growing trend toward monetary compensation sought for non-monetary damages, may not set a precedent in a broad sense because of the government’s sovereign immunity, the legal doctrine immunizing the government from liability in cases of ambiguity, experts say.
Though the government-as-defendant makes the impact of the ruling less significant in this case, the case could have a stronger persuasive value when it comes to state laws, according to Ann Waldo, CIPP/US, of Wittie, Letsche & Waldo.

“Since Congress didn’t make the Privacy Act clear in explicitly allowing damages for nonpecuniary injuries, the court said that this had to be construed narrowly,” Waldo said. “The holding unquestionably relied on (the justices’) perceived sense that they were compelled to limit actual damages narrowly because of the very strong canon of statutory interpretations.”

“With respect to claims of Privacy Act breaches against the government, the court has made it difficult to assert those claims,” agreed InfoLawGroup’s Dave Navetta, CIPP/US. He said that although the Cooper case may have a limited impact on future holdings, its outcome isn’t rare, adding that, in general, plaintiffs have struggled to allege harm because of the law’s narrow scope. Even time lost or the cost of credit monitoring are “damages that are typically not recognized in a court of law” and are often dismissed.

“I think plaintiffs in many cases may have the facts in their favor, but the law, in terms of harm, is very much not in their favor,” he said.

However, Navetta said high-profile cases where loss of data has occurred and a brand’s reputation is at risk may be more likely to be settled.

“With brand-name companies, even if it looks like cases are going to be dismissed early on the ‘harm’ issue, there’s still some risk involved. I think defendants look at them differently than smaller breaches where the risk may not be as great,” he said.

Carnegie Mellon researchers found that breaches that have occurred due to “unauthorized disclosure or disposal” of data are twice as likely to result in lawsuits than those due to hacking incidents and that financial loss and proof of harm were determining factors in whether companies settled suits.

Navetta points to the Hannaford Brothers data breach of 2007, in which millions of payment card numbers were exposed and fraudulent charges placed. A First Circuit Court in Maine ruled that victims could recover costs incurred when they purchased credit insurance or new identity theft monitoring—cognizable harms.

In September 2011, however, a U.S. District Court judge dismissed a group of consolidated class-action suits alleging that Apple and eight mobile-application makers shared users’ personal information without their consent, writing in her opinion that the plaintiffs did not show any tangible injuries.

In FAA v. Cooper, the defendant argued that while Cooper may have suffered an “adverse effect,” he didn’t necessarily suffer “actual damages.” One justice said Congress likely did intend the Privacy Act to cover emotional distress suits, but in the end, the majority disagreed.

Simon Frankel of Covington and Burling agrees that the question at hand is how lower courts will apply the Cooper ruling to other cases.

“Will lower courts interpret Cooper narrowly to mean that ‘actual damages’ is limited to monetary harm where it allows monetary relief against the government, acting as a waiver of sovereign immunity, or treat it as a broader holding that when statutes allow for actual damages, they only allow for recovery of monetary harm and not emotional distress or damages or reputational damages,” he said. “That’s what I think is the difficult open question.”
Mali Friedman, also of Covington and Burling, said the Cooper holding is representative of a tactic frequently used by plaintiff’s counsel, “which is to allege emotional harm and other types of damages that simply aren’t cognizable under certain statutes.”

Friedman said courts also have yet to attach the same value to personal data that plaintiffs deem it to have.

“No court has yet held that the collection or disclosure of an individual’s data has any cognizable economic value to that individual. Of course, personal data in the aggregate often has value to a company, but courts repeatedly have found that there is no compensable loss where an individual’s information is collected or shared.”

Dr. Deborah Peel, a physician and health privacy advocate, says the implications of Cooper are significant from a health privacy standpoint.

“Emotional injuries are real and they cause great harm,” said Peel. “All you have to do is think about post-traumatic stress disorder in the military.

She said the FAA and SSA’s actions in comparing personal data send a daunting message to Americans asked to disclose sensitive data to government agencies, such as Cooper’s HIV status, and those messages can have repercussions.

“Where you have situations where reporting a condition is going to destroy livelihood, reputation or future, many people will not seek medical treatment. Cooper counted on the Privacy Act to keep his records private, and it didn’t.”

As the U.S. healthcare system moves towards electronic health records, Peel said it’s “incredibly important that we move toward systems that are trusted. How can we ask the public to participate in these systems when they don’t even know where the data goes?”

Waldo said she expects the case could raise issues regarding future government data sharing.

“This was only in 2002,” she said of the agencies’ investigation into Cooper. “In 2012, there are many efforts—and in the next decade, I predict far more efforts—to make government more modern, integrated and data-interoperable. As that goes on, I think many people can expect some unwelcome surprises from government...Increasingly, government will become far more efficient and aggressive in achieving that data interoperability.”

As an example, Waldo noted strong efforts to connect state databases on prescription drug abuse for law enforcement purposes.

In the end, Morrison and Foerster’s Freeman said that although plaintiffs now struggle to collect harm damages, there’s time yet.

“There’s some possibility that the inability of consumers to have their day in court for the perceived privacy violations could spark Congress or state legislatures to respond with a new law that remedies that problem,” he said.
The global privacy landscape is experiencing its largest shift since the implementation of the European Union’s adoption of Directive 95/46/EC in 1995. The directive was foundational in establishing a privacy regime in Europe, with a global ripple effect for countries wishing to transfer data to and from the EU; examples include the enactment of the Personal Information Protection and Electronic Documents Act in Canada and negotiations between the U.S. and the EU resulting in the Safe Harbor agreement.

Many papers and initiatives in the last few years have paid more attention to the concepts of transparency and accountability. In March of 2012, the U.S. Federal Trade Commission issued a final staff report, “Protecting Consumer Privacy in an Era of Rapid Change: a Proposed Framework for Businesses and Policymakers,” calling for organizations to implement Privacy by Design into every stage of the development of products and services—shifting the burden away from consumers and placing obligations on businesses to treat consumer data in a responsible manner—and recommended that companies increase transparency of their data-handling practices by means of shorter and clearer privacy notices, reasonable access and providing education to consumers about commercial data privacy practices. The proposed European Commission Regulation on the Protection of Individuals with Regards to the Processing of Personal Data, released in January, requires that data controllers adopt policies and implement measures to be able to demonstrate that processing of personal data is performed in compliance with the regulation, maintain documentation of all processing operations under their responsibility and incorporate the concepts of data protection by design and default.

Canadian privacy commissioners’ paper: The next leap forward

In April, the Canadian federal privacy commissioner and the information and privacy commissioners of Alberta and British Columbia issued a paper, “Getting Accountability Right With A Privacy Management Program,” which significantly “moved the yardsticks” for Canadian organizations. The commissioners noted that in relation to privacy, accountability is the “acceptance of responsibility for personal information protection” and that accountable organizations must be able to “demonstrate to privacy commissioners that they have an effective, up-to-date privacy management program in place.” The ability to demonstrate—or attest—that the organization not only has a privacy management program but one which is effective and updated is an important step forward within the global privacy framework.

The commissioners’ paper identifies the building blocks companies need to put in place to be “accountable” organizations, including organizational commitment; i.e., buy-in from the top, appointment of a privacy officer and a privacy office where appropriate and internal reporting mechanisms; program controls such as a personal information inventory; internal policies that give effect to the privacy principles; conducting risk assessments; ongoing training and awareness for employees; a breach management protocol; management of service provider by means of contracts, and external privacy notices. An accountable organization must also, on an ongoing basis, assess and revise its privacy management program, including the program controls.
The above steps, where fully implemented, allow an organization to demonstrate to all relevant stakeholders, including customers, employees, privacy commissioners, etc., that it has a privacy program in place. As noted in the commissioners’ paper, “During an investigation or audit, our offices will expect that organizations can demonstrate that they have an up-to-date, comprehensive privacy program in place.” Whether or not an organization has such a program in place will inform the commissioners’ decisions as to whether the organization has reasonable safeguards in place and is complying with the accountable requirements or if the organization will require additional work to create—or update—such a program.

**John Jager, CIPP/C, CIPP/US, is vice president of research services at Nymity, Inc., which offers web-based privacy support to help organizations control their privacy risk. He may be reached at john.jager@nymity.com.**
EU—Article 29 Working Party publishes biometrics opinions

By Jan Dhont and Katherine Woodcock

On March 22 and April 27, the Article 29 Working Party published two opinions on biometrics, one relating to facial recognition in online and mobile services (Opinion on Facial Recognition) and a second on developments in biometric technology (Opinion on Biometrics). Both opinions build on the Working Party's Working Document on Biometrics and seek to provide greater guidance to authorities, the biometrics industry and users alike.

The Opinion on Biometrics, which deals with the broader category of biometric technology—interestingly, published after the Opinion on Facial Recognition—sets out the basis legal framework for the implementation of biometric technology. It focuses on the clarity of purposes—and notice—for processing biometric data, the protection of fundamental rights of the data subject and ensuring that alternative means are available for data subject to choose should they not wish to have their biometric data processed. This is particularly emphasized in tandem with consent as a legal basis for processing; less privacy-intrusive mechanisms should be made available to permit individuals to have real choice to consent to biometric processing. The Working Party highlights this, specifically, within the context of employment, where freely given consent is often questioned.

The Opinion on Facial Recognition discusses the instances when digital images qualify as personal and sensitive data as well as the legitimate grounds for processing this personal data. One point which is highlighted is that consent from the image uploader should not be confused with the necessity of legitimate grounds for processing other individuals who may also be in the image. Here, a data controller will likely need to rely on its legitimate interests and sufficient balance these against the fundamental rights and freedoms of the data subjects.

Both opinions present detailed definitions relating to biometric technology and practical examples of how biometric personal data should—and should not—be utilized in practice. In light of the rapidly evolving technology and use of biometrics, these opinions set the framework on how to implement biometrics and what steps should be taken to properly protect the processing of personal data within such processing. This will provide companies and business, including online and mobile device companies, with detailed guidance on the use of biometrics in the European Union.

The full text of the Opinion on Facial Recognition is available here and the full text of the Opinion on Biometrics is available here.

Jan Dhont heads the privacy practice of Lorenz Brussels. He specializes in data protection and privacy, telecommunications, media and technology law. He may be reached at j.dhont@lorenz-law.com.

Katherine Woodcock is an attorney with Lorenz Brussels. She may be reached at k.woodcock@lorenz-law.com.
FRANCE—Implementation decree on data breaches

By Pascale Gelly, CIPP/E

Six months after the adoption of the ordinance implementing the 2009 e-Privacy Directive in August 2011, the implementation decree has finally been adopted.

The decree brings precision about the means and the content of the notification obligation. The notification to the CNIL must be made by letter provided against signature and specify the nature and consequences of the breach, the measures taken or contemplated to remedy the breach, the people to contact to obtain additional information and, if possible, an estimate of the number of impacted individuals.

The service provider is free to use any means to provide the notification to individuals as long as it can provide evidence of having done so. It must describe the nature of the data breach, the people to contact to obtain more information and the measures recommended to limit the adverse effects of the breach.

The decree specifies under which conditions the service provider can be exempted from the obligation to notify individuals. The CNIL must have considered that the service provider has efficiently applied appropriate protective measures which make the data unintelligible to any person not authorized to access it. The service provider must provide the CNIL with a complete record including, in particular, a description of the measures and of the steps taken to make them effective. If within two months the CNIL has not provided an opinion, then it is considered as negative and the service provider must notify the individuals.

The authority may also, in case of a serious breach, order the service provider to notify the individuals within a month.

Pascale Gelly, CIPP/E, of the French law firm Cabinet Gelly, can be reached at pg@pascalegelly.com.
FRANCE—2012: Increase of CNIL investigations to come

By Pascale Gelly, CIPP/E

Video surveillance, the healthcare sector, smartphones, sports, data security, large data files—police, highways, gas, electricity—these are the targets selected this year by the French data protection authority (CNIL) as justifying specific attention in its enforcement programme.

The CNIL mission is to ensure compliance with the French data protection law of January 6, 1978. To this goal, it performs onsite investigations on the premises of businesses and government bodies in order to verify whether the personal data they handle about customers, employees, citizens, patients, etc., are duly processed in compliance with the rules of the law on the protection of privacy and personal data.

Many investigations are triggered by complaints or scandals revealed by the media. However, a large part of the controls operated by the CNIL are based on an annual programme which is set every year in the spring where the CNIL identifies objectives and priorities. The authority keeps intensifying its enforcement activity. Whereas in 2010, 318 investigations were made, the 2012 objective is 450 investigations.

This spring, the authority decided to pursue its vigilance effort on video surveillance activities, begun two years ago, which bring it regularly to publicize excessive surveillance practices over employees or within schools.

It recently sanctioned a host provider of health data for not having complied with its security commitments. The data was not encrypted. Host providers are on the CNIL’s radar screen in particular in light of the issues raised by cloud computing. More generally, health data and its security are a topic of concern and interest, as are health-related applications on the Internet, the patient medical record, the pharmaceutical record and clinical research.

The 2011 investigation programme included the topic “Internet tracking.” In 2012, the CNIL both refines and broadens the topic as it looks at all data processing carried out around smartphones: Who knows what about the subscriber, who subscribes to a smartphone offer and then makes use of all its functionalities, in particular by downloading apps.

Although Paris has not been selected to host the Olympics this year, the CNIL has decided to keep a place for sports and games in its investigation programme. It announces investigations of stadiums and sport organizations on data processing relating to attendants, licensees and a special interest for black lists and anti-doping.

A summary of the investigation programme is available in French on the CNIL website.

Pascale Gelly, CIPP/E, of the French law firm Cabinet Gelly, can be reached at pg@pascalegelly.com.
GERMANY—Regional Court of Berlin on expiry date of consent

By Flemming Moos

In its judgement of 9 December 2011, the Regional Court of Berlin (Case No. 15 O 343/11) had to decide on the permissibility of a certain e-mail advertising campaign. While after several decisions by the Federal Court of Justice, it is settled case law that an opt-in is generally required for e-mail marketing measures and that such an opt-in must be “separate” in the sense that it may not extend to other marketing forms such as telephone calls or telefax messages, the Berlin judges were, in this case, also called to rule upon the questions whether the consent was specific enough and whether it was still valid.

The judges held that, in this case, the declaration of consent did not meet the legal requirements. They were of the opinion that for consent to be valid, it must only refer to a specific electronic marketing measure of a specified company. Here, the defendant had only obtained a “general consent” which basically allowed “any kind of marketing e-mails by an unlimited number of companies from various economic sectors.”

Also, the court found the declaration of consent to be outdated. It ruled that consent may only justify e-mail marketing measures for a certain period of time. After a period of one-and-a-half years, however, as in the case at hand, the consent would have become void because, according to the judges of the Regional Court of Berlin, the consent would no longer refer to the “specific case.”

The judgement illustrates the importance of complying with the high demands on valid declarations of consent in Germany. Businesses should not only carefully draft the declarations but also have in place a proper opt-in management system.

Flemming Moos is a partner at Norton Rose in Germany and a certified specialist for information technology law. He chairs the IAPP KnowledgeNet in Hamburg and can be reached at flemming.moos@nortonrose.com.
ISRAEL—Proposed guide on workplace privacy

By Dan Or-Hof, CIPP

The Israeli Law Information and Technology Authority (ILITA) has published a consultation draft guide on protecting personal information in workplace environments.

The purpose of the proposed guide is to reflect ILITA's view of the principles applicable to the right of privacy in personal information that employers store and process and recommend adequate practices to implement these principles.

The guide is not obligatory. However, it reflects ILITA's interpretation of the law. Once formally released, the guide will serve as a basis for ILITA's enforcement activities in workplace environments.

Six main practices are particularly recommended under the proposed guide: review the data collected by the employer throughout the employment term and the purposes of data collection; identify and map the stored data, the data's use and manage access to the data; maintain adequate information security rules, procedures and mechanisms; provide appropriate guidance to relevant personnel; maintain close supervision on outsourcing services, and set an explicit and clear policy that covers the permitted use of the computer systems by employees and the employer's ability to monitor such use.

The guide is comprised of three chapters. The first introduces the general principles for collecting and processing personal information. Among these rules are the need to receive the employee's informative and freely given consent to the processing of the employee's information, to process the data for merited purposes and to the extent no greater than required, to provide adequate transparency of the employer's privacy practices, to avoid processing data otherwise than for the purpose for which the data was collected, to maintain confidentiality and security of the data, to allow employees access and the right to amend their personal information and to monitor outsourcing services through adequate contractual requirements and audits.

The second chapter provides a deeper look into the practices of data management and divides the data lifecycle to three phases. It begins with the proper procedures for managing the personal information of job applicants, including job interviews, information that the employer cannot request—such as genetic data, military profile, religion, sexual orientation, etc., and the employer's relations with job placement services.

The next phase is the management of the employee's file. This section covers ongoing data collection about the employees, the principles for maintaining an employee database, information security practices and the required data-mapping process.

The last data cycle phase discusses proper data retention practices.
The third chapter of the guide provides ILITA’s insights about the regulation of monitoring technology. ILITA relies, in that regard, on an opinion delivered last year by the National Labor Court that laid down a comprehensive set of rules on employers' rights to monitor their employees. According to the opinion, every employer must form an adequate policy that covers the boundaries of permitted use of the employer's computer systems—including e-mail, applications and telephone usage, provide a clear understanding about the employer's monitoring practices and receive the employees' consent to the policy.

ILITA requests the public to comment on the proposed guide until June 17. Israeli employers and international corporations that operate in Israel should review the proposed guide and assess the impacts of its provisions on their privacy practices. While some of the provisions are already implemented by many employers, others will need to allocate additional attention and resources to meet the guide's requirements.

A copy of the guide, in Hebrew, is available on ILITA's website.

Dan Or-Hof, CIPP, is a New York and Israeli attorney, a partner and the manager of the IT, Copyright and Internet Team at Pearl Cohen Zedek Latzer with specific practice in data protection and privacy law.
UK—ICO grace period for compliance with new cookie rules comes to an end

By Leonie Power

The new EU rules on cookies came into force in the UK on 26 May 2011, but the Information Commissioner’s Office (ICO) indicated that it would implement a grace period of one year to allow businesses to comply. The 12-month grace period will expire this month, and it seems likely that some businesses will still be caught out.

While fines are unlikely, businesses should not assume that noncompliant websites will not be subject to some kind of enforcement action. It is likely that the ICO will focus on ensuring that infringing sites take steps to comply within a limited time period and will make full use of its powers to issue undertakings and enforcement notices.

Businesses that are still wondering what to do should take action as soon as possible to avoid regulatory scrutiny. Steps to take include auditing your cookie use to find out what you have got; assessing the intrusiveness of your cookies; adopting a notice-and-consent strategy appropriate to the intrusiveness of your cookies, and implementing forward-facing cookie management mechanisms.

International Chamber of Commerce UK publishes new guide on complying with cookie rules

As the 12-month amnesty for compliance with new cookie rules comes to an end, the International Chamber of Commerce UK (ICC) has published a guide to help organizations to comply with the rules.

The guide categorizes cookies into four different types: strictly necessary cookies, performance cookies, functionality cookies and targeting or advertising cookies, although the guide makes clear that this categorization may be subject to change.

Part II of the guide provides information about each category of cookie, the aim of which is to assist website users in understanding how particular types of cookies are used. Part III of the guide consists of technical guidance for website operators to assist them in understanding what cookies are used on their websites and in categorizing such cookies. Part IV contains some suggestions for obtaining consent from website users in relation to each category of cookie. The guide makes clear that Part IV is based on current guidance issued by the ICO but is not intended to be prescriptive.

The ICO has said that the ICC’s guide compliments the ICO’s existing cookies guidance. The ICO has also indicated that it will be updating its own cookies guidance before the end of the 12-month grace period to ensure the sharing of best practice advice.

Leonie Power is a senior associate with Field Fisher Waterhouse and a member of the firm’s Privacy and Information Law Group. She can be reached at leonie.power@ffw.com.
UK—ICO issues monetary penalty to a Welsh health board

By Leonie Power

The Information Commissioner's Office (ICO) has issued a monetary penalty of £70,000 to a Welsh health board following an incident in March last year in which a patient's health details ended up in the wrong hands.

The ICO found that the staff members involved in the data breach had not received data protection training and that adequate procedures were not in place to ensure that the information was not misdirected.

The health board is the first National Health Service (NHS) organization to be served with a monetary penalty. The ICO drew attention to the sensitive nature of information held by the health service and called on NHS organizations to take notice of its decision in order to avoid future enforcement action.

Leonie Power is a senior associate with Field Fisher Waterhouse and a member of the firm’s Privacy and Information Law Group. She can be reached at leonie.power@ffw.com.
Company offers two EU compliance management tools

As businesses and organizations prepare for upcoming reforms to the EU data protection framework and potential enforcement of the ePrivacy Directive in the UK, TRUSTe has announced it is offering a suite of tools to help manage these new compliance obligations.

In conjunction with its recently released EU Cookie Audit and under the umbrella of its EU Privacy Management Suite, the privacy management solutions provider has released TRUSTed Consent Manager to help organizations address new privacy management challenges posed in the EU. For websites visited by EU consumers, the consent management system helps organizations meet the informed consent requirement in the EU data protection directive and the May 25 deadline set forth by the UK for compliance. According to TRUSTe, the consent manager can be easily implemented by a website operator while also providing consumers with transparency and choice about the site’s data collection and use policies. For flexibility in working with different international regulations, the consent management system offers both express and implied consent mechanisms for increased adaptability.

TRUSTed Ads EU, TRUSTe’s second compliance management release, is designed to help advertisers, publishers and networks using online behavioral advertising to meet the privacy standards put forth in the European Self-Regulatory Framework for Online Behavioral Advertising—a set of standards created by the IAB Europe and EASA. The system also offers the globally recognized “Forward I” Advertising Option Icon.

TRUSTe EMEA Managing Director Danilo Labovic said his team is “partnering with UK and European companies as they strive to implement privacy programs that better reflect their own high standards of customer care while complying with regulatory changes.”

—IAPP Staff
Collaboration produces universal privacy tool for cookie compliance

With cookie enforcement on the horizon in the UK and eventually throughout Europe, two companies have teamed up to provide website owners with a way to achieve cookie compliance while providing users with a consent tool to transmit tracking preferences.

The online tool stems from a partnership between TagMan and Evidon “to enable clients to deploy the most comprehensive privacy and compliance solution from within the TagMan system.”

Since 2007, TagMan has allowed website owners to add, edit or remove onsite tracking tags, including site analytics, display ad serving, search, e-mail, affiliate and social media. As a result, website owners have been able to control tags and cookies directly.

Now, on top of TagMan’s management system is Evidon’s “privacy layer,” which provides clients with a consent tool. This tool lets website visitors see the companies that are placing cookies and other tracking tools on their computer. The new tool also gives the visitor a channel to indicate their data collection preferences--“a key component of compliance with the ePrivacy Directive.”

TagMan CEO Paul Cook said Evidon “has a proven track record in developing platforms that help businesses to comply easily with privacy laws and self-regulatory programmes. This partnership enables us to combine the best of both systems and offer a highly sophisticated, integrated privacy tool for our clients.”

Evidon CEO Scott Meyer added, “Control of third-party marketing tags is crucial for website owners to comply with the ePrivacy Directive and other privacy regulations around the globe...this collaboration will ensure that (TagMan's) clients have access to the tools necessary to become fully compliant with the EU ePrivacy Directive and the U.S. FTC guidance.”

—IAPP Staff
Seeking members’ input

Your answers to four questions will help the IAPP tailor its content offerings.

The IAPP provides a variety of content offerings for members, including a website, news and feature articles, web conferences, research reports, live events, books and other offerings. Occasionally we like to check in with members to ensure that we are providing the content you want and need. Your answers to this four-question survey will help us identify ways to continuously improve our offerings for your benefit.

Thank you in advance for sharing your preferences.

Take the four-question survey.

IAPP Board Chairman and Royal Bank of Canada Vice President Global Compliance and Chief Privacy Officer Jeff Green, CIPP/C, speaks at the IAPP Canada Privacy Symposium held in early May in Toronto.

View Photos
(Must be a Facebook user and logged in to view.)