29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Séance d'information
Dragon : *La mondialisation*
« À qui faites-vous confiance?
Un regard sur les sceaux de confidentialité »

Information Session
"*Globalization*" Dragon
"Who Do You Trust?
A Look At Privacy Seals"

27 septembre/September 27
13h30 – 14h30

Série Terra Incognita, cahier de travail # 11/Terra Incognita, workbook series # 11

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Table des matières / Table of contents

Biographies

Présidente : M^me^ Christine A. Varney

En 1997, Christine Varney s'est de nouveau jointe à Hogan & Hartson (Washington) à titre d'associée. Elle était chargée de diriger le groupe du cabinet qui s'occupait des pratiques liées à Internet. Ce groupe offre aux entreprises faisant des affaires à l'échelle mondiale une gamme complète de services, notamment des conseils sur la législation antitrust, la protection de la vie privée, la planification opérationnelle et la gouvernance d'entreprise, la propriété intellectuelle et les questions d'ordre général liées aux responsabilités. M^me^ Varney fournit aussi des conseils sur la législation antitrust, les politiques et la réglementation en matière de concurrence à diverses entreprises. Parmi celles-ci, on peut mentionner eBay, Fox Interactive Media/ MySpace, Ernst & Young, Zango, DoubleClick, le *Washington Post, Newsweek* Interactive, Dow Jones & Company, AOL, Synopsys, Compaq Computer, Gateway, Netscape, The Liberty Alliance, Online Privacy Alliance et Real Networks. Avant de se joindre de nouveau à Hogan & Hartson, M^me^ Varney était l'adjointe du président et la secrétaire du Cabinet, et elle a occupé le poste de déléguée commerciale fédérale de 1994 à 1997.

Conférencières

Me Kirsten Bock

M^e^ Bock (juriste) a étudié le droit à l'Université de Kiel et à l'Université de Surrey, au Royaume-Uni. Elle s'est jointe au Independent Centre for Privacy Protection Schleswig-Holstein (Centre indépendant pour la protection de la vie privée) en 2004, où elle coordonne les projets internationaux du gouvernement en direct. À titre de gestionnaire principale de projet, elle est responsable des projets eTEN suivants : RISER (Service de registre des renseignements sur les citoyens européens), IM enabled (Service d'intégration des technologies de la GI aux services du gouvernement en direct) et EuroPriSe (Sceau européen de la protection de la vie privée). Elle a donné des conférences à l'Université des sciences appliquées de l'administration et des services d'Altenholz et à l'Université des sciences appliquées de Kiel.

Biographies

Chair : Ms. Christine A. Varney

In 1997 Christine Varney rejoined Hogan & Hartson (Washington) as a partner to head the firm's Internet practice group. This practice provides full service assistance to companies doing business globally, including advising on antitrust, privacy, business planning and corporate governance, intellectual property, and general liability issues. Ms. Varney also provides antitrust, competition policy and regulatory advice to a variety of companies. Among them are eBay, Fox Interactive Media/MySpace, Ernst & Young, Zango, DoubleClick, *Washington Post, Newsweek* Interactive, Dow Jones & Company, AOL, Synopsys, Compaq Computer, Gateway, Netscape, The Liberty Alliance, Online Privacy Alliance and Real Networks. Before rejoining Hogan & Hartson, Ms. Varney was an assistant to the President and secretary to the Cabinet, and served as a federal trade commissioner from 1994 to 1997.

Speakers

Ms. Kirsten Bock

Ms Bock (Ass. Jur.) studied Law at the Universities of Kiel and Surrey, UK. She joined the Independent Centre for Privacy Protection Schleswig-Holstein (ICPP) in 2004 where she is Coordinator for International e-Government Projects. As Senior Project Manager, she in charge of the eTEN projects RISER: Registry Information Service on European Residents, IM enabled: A Service to Facilitate the IM Enabling of eGovernment Services, and EuroPriSe: European Privacy Seal. She has lectured at the University of Applied Science for Administration and Services Altenholz and the University of Applied Science Kiel.

M^{me} Fran Maier

Fran Maier est la directrice générale et la présidente de TRUSTe, qui domine dans le secteur de la protection de la vie privée sur Internet. M^{me} Maier a plus de 15 ans d'expérience dans l'établissement de marques de consommation et dans le renforcement de la confiance des consommateurs. Elle est reconnue pour son expertise dans les domaines de la protection de la vie privée et des pratiques exemplaires dans le marketing sur Internet ainsi que du marketing s'adressant aux femmes. En tant que cofondatrice de Match.com, elle a établi la crédibilité et la sécurité de cette entreprise, en faisant de ce site une agence de rencontre digne de confiance. Match.com est devenu le site de rencontre préféré des femmes célibataires. Dans ses fonctions de direction du marketing chez Women.com et la filiale BlueLight.com de Kmart, M^{me} Maier a créé de nouvelles marques en ligne et fait en sorte que des marques hors ligne sûres soient offertes sur Internet. M^{me} Maier a obtenu un baccalauréat et une maîtrise en administration des affaires à l'Université Stanford.

Ms. Fran Maier

Fran Maier is the Executive Director and President of TRUSTe, the leading brand in online privacy. Ms. Maier brings more than 15 years experience building consumer brands and enhancing consumer trust. She is known for her expertise in online privacy, online marketing best practices, and marketing to women. As a co-founder of Match.com she established credibility, safety and trust in online dating, making Match.com the favorite dating site for single women. In executive marketing roles at Women.com and Kmart's BlueLight.com subsidiary, Ms. Maier has established both new start-up online brands and brought blue-chip offline brands onto the Internet. Ms. Maier holds a BA and MBA from Stanford University.

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

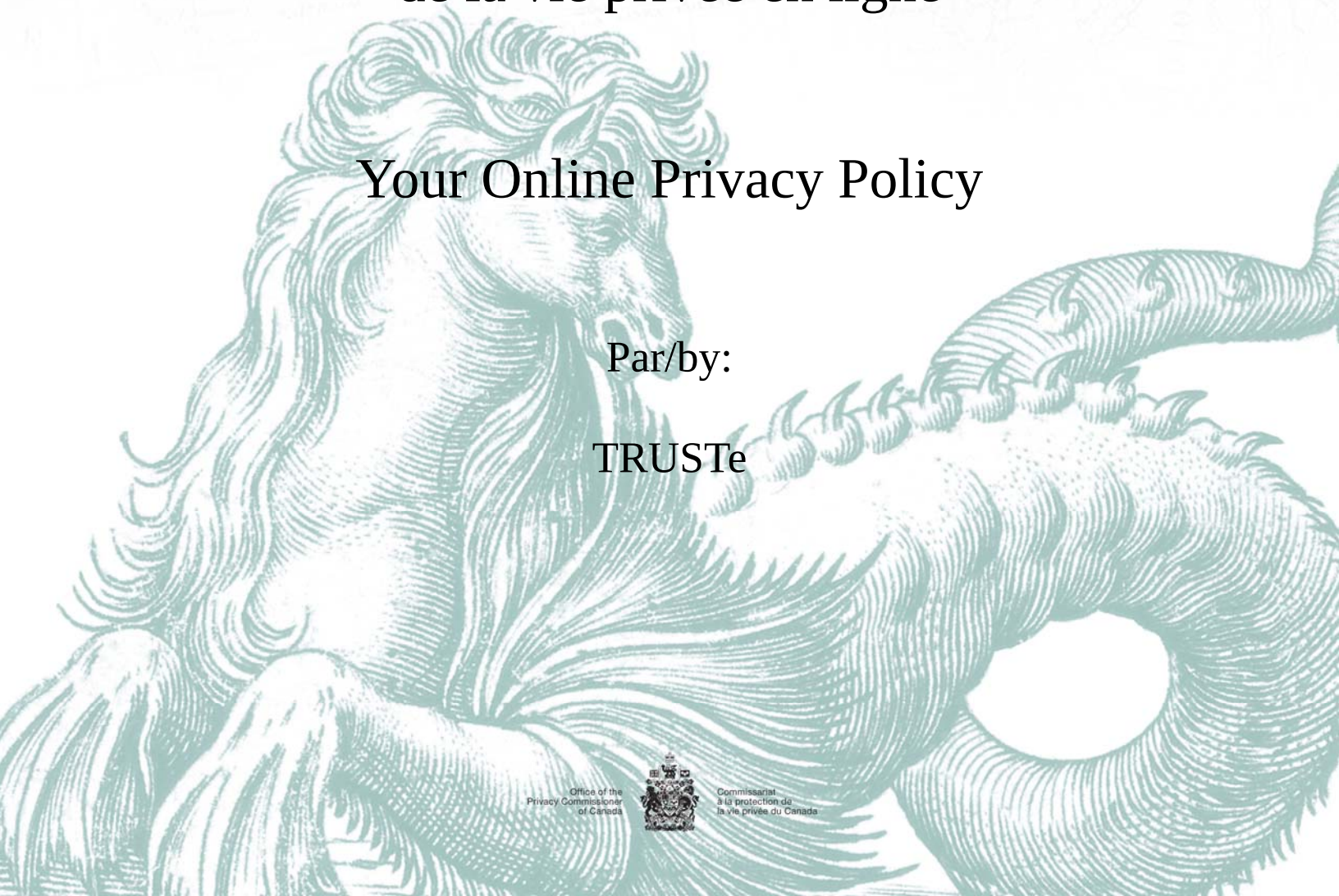
29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Votre politique sur la protection de la vie privée en ligne

Your Online Privacy Policy

Par/by:

TRUSTe



Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

« Bien conçu, votre énoncé de protection de la vie privée est un outil de communication précieux qui peut contribuer à la confiance que vos clients placent en vous. Cette confiance vous aidera à protéger votre marque de commerce et à soutenir la concurrence féroce des marchés en ligne.» [Traduction]
Bennie Smith, chef de la protection des renseignements personnels de *Doubleclick*

Qu'est-ce qu'un énoncé de protection de la vie privée?

Un énoncé de protection de la vie privée est un outil qui permet à l'entreprise d'expliquer à ses clients comment elle utilise leurs renseignements personnels. Les entreprises ont évidemment toutes sortes de politiques qui les guident dans leur administration des renseignements personnels, mais le présent guide ne traite que des énoncés de protection de la vie privée à afficher en ligne à l'intention du public. Ces énoncés ont cela de particulier qu'ils s'adressent uniquement au public. N'importe qui peut les lire, en tout temps, et ils s'appliquent à tous ceux qui visiteront le site Web sur lequel ils paraissent.

Les énoncés de protection de la vie privée peuvent prendre toutes sortes de formes. Il n'existe pas, à l'heure actuelle, de norme industrielle qui favorise une formule plutôt qu'une autre dans le cyberespace. Certains énoncés sont de longs textes téléchargeables en format PDF, d'autres sont de simples avertissements d'un paragraphe, présentés dans une fenêtre flash. Les sites Web ont tous leur spécificité, dont les énoncés de protection de la vie privée doivent témoigner en expliquant les pratiques de collecte et de traitement des données qui leur sont propres.

Les pratiques équitables de traitement des renseignements que propose la Federal Trade Commission (FTC) ne constituent pas tout à fait une norme industrielle des pratiques de protection de la vie privée en ligne, mais elles s'en rapprochent beaucoup. Elles s'inspirent des principes de bonne gestion de l'information sur lesquels reposent les démocraties responsables. Plus précisément, elles s'appuient sur l'idée qu'un consommateur doit comprendre parfaitement la manière qu'a une entreprise de traiter et d'utiliser l'information pour décider en toute connaissance de cause s'il veut ou non lui communiquer ses renseignements personnels.

"Crafted correctly, your privacy statement is a meaningful communication that can build consumer trust and confidence. This trust will help protect your brand and its underlying promise from the ravages of the highly competitive online marketing space. "
Bennie Smith, chief privacy officer, *Doubleclick*

What is a Privacy Statement?

A privacy statement is a communication to consumers about how a company uses their personal information. Although businesses of all sorts create privacy policies, this paper focuses solely on public-facing privacy statements posted online. These statements are unique in that they are wholly public: they can be viewed by anyone, at any time, and apply to anyone visiting the Web site on which they are displayed.

Privacy statements come in many shapes and sizes. There is no current industry standard in the online community about what privacy statements should look like. Some take the form of lengthy, downloadable PDFs while others are simple disclaimers presented in a one-paragraph pop-up window. Every Web site is unique and a privacy statement must reflect a site's unique data-handling and collection practices.

The Federal Trade Commission's Fair Information Practices are the closest thing the industry has to an online standard for privacy practices. The Fair Information Practices are based on the principles of full diclosure that underlie an enlightened democracy. Specifically, only when consumers have a full understanding of how an organization maintains and uses information can they make informed decisions regarding the disclosure of their personal information.

The Fair Information Practices

- **Notice.** Web sites should provide full disclosure of what personal information is collected and how it is used.
- **Choice.** Consumers at a Web site should be given choice about how their personal information is used.
- **Access.** Once consumers have disclosed personal information, they should have access to it.
- **Security.** Personal information disclosed to Web sites should be secured to ensure the information stays private.

Les pratiques équitables de traitement des renseignements

- **Avis.** Les sites Web qui recueillent des renseignements personnels doivent indiquer clairement qu'ils le font et comment ils utilisent ces renseignements.
- **Choix.** Les consommateurs qui visitent un site Web doivent pouvoir choisir comment seront utilisés leurs renseignements personnels.
- **Accès.** Une fois que les consommateurs auront communiqué leurs renseignements personnels, ils doivent pouvoir y accéder.
- **Sécurité.** Les renseignements personnels fournis sur un site Web doivent être protégés de manière à en préserver la confidentialité.
- **Recours.** Les consommateurs doivent disposer d'un moyen qui leur permet de résoudre les problèmes que pourrait poser l'utilisation ou la communication de leurs renseignements personnels sur un site Web.

Pourquoi afficher un énoncé de protection de la vie privée?

Les énoncés de protection de la vie privée inspirent confiance aux consommateurs. Ils leur indiquent que l'organisation à qui appartient le site se soucie des préoccupations que peuvent avoir les consommateurs à propos de leurs renseignements personnels et qu'elle a pris le temps d'évaluer ses pratiques en la matière et d'établir une façon de procéder qui protège les renseignements personnels.

Depuis quelques années, les consommateurs se montrent plus exigeants en matière de protection de la vie privée. Des études montrent qu'ils sont de moins en moins nombreux à penser que les entreprises traitent leurs renseignements personnels avec tout le soin nécessaire. En même temps, le public a de moins en moins le sentiment que les lois en vigueur assurent un niveau de protection raisonnable de la vie privée[1].

Les énoncés de protection de la vie privée ont pour effet d'apaiser les inquiétudes des consommateurs. Plus de 80 p. 100 des consommateurs en ligne lisent les énoncés de protection de la vie privée des sites et les quelque 20 p. 100 qui restent signalent que même un court résumé des pratiques d'un site en matière de protection de la vie privée les rassure[2].

- **Redress.** Consumers should have a way to resolve problems that may arise regarding sites' use and disclosure of their personal information.

Why Post a Privacy Statement?

Privacy statements build consumer confidence. A privacy statement signals to consumers that a site respects their privacy concerns and has taken the time to evaluate its privacy practices and institute procedures to protect personal information.

Consumer attitudes toward privacy issues have become tougher in recent years. Studies reveal that fewer people trust businesses to handle consumers' personal information in an acceptable way. At the same time, fewer people put faith in existing laws to provide reasonable levels of privacy protection.[1]

Privacy statements help to allay consumer anxieties significantly. More than 80 percent of online consumers have read a site's privacy statement and the remaining percentile report that even a short summary of a site's privacy practices make them feel more secure online.[2]

When consumers believe a site is trustworthy, they are more likely to engage in valuable online activities, such as making purchases, clicking on ads, disclosing personal information, filling out surveys for market research, contributing content, downloading software, and returning to the site in the future.

> "If your company plays in a privacy-sensitive industry, your customer databases may be empty in a few years if you don't start investing in privacy now. If customers can't see the results of the investment, privacy won't pay." *Computerworld*, 2003

You may be required to post a privacy statement. In recent years, a number of privacy laws have been enacted, forcing many companies to play catch-up in the privacy arena or face steep fines and lawsuits.

Quand des consommateurs jugent un site fiable, ils ont davantage tendance à participer à ses activités en ligne importantes, par exemple à y faire des achats, à cliquer sur les publicités, à communiquer leurs renseignements personnels, à répondre aux sondages réalisés en vue d'études de marché, à fournir du contenu, à télécharger des logiciels et à retourner sur le site par la suite.

> « Si votre entreprise œuvre dans une industrie qui repose sur les renseignements personnels, votre base de données sur vos clients pourrait bien se vider dans les prochaines années si vous ne commencez pas bientôt à investir dans la protection de la vie privée. Et si les consommateurs ne voient pas les résultats de vos investissements, vos efforts n'auront servi à rien. » [Traduction] *Computerworld*, 2003

Les lois qui protègent la vie privée

Les entreprises de services financiers doivent afficher un énoncé de protection de la vie privée qui décrit les mesures de protection des données qu'elles prennent aux termes de la Gramm-Leach-Bliley Act (GLBA).

Les sites pour enfants doivent obtenir un consentement vérifiable des parents avant de recueillir de l'information sur leurs enfants aux termes de la Children's Online Privacy Protection Act (COPPA).

Les sites d'entreprises qui font affaire avec l'Union européenne doivent respecter la Directive de l'Union européenne sur la protection des données qui réglemente la collecte, l'utilisation et la protection des renseignements personnels des citoyens de l'Union européenne.

Les sites d'entreprises médicales ou de compagnies d'assurance sont assujettis à la Health Insurance Portability and Accountability Act (HIPAA) qui régit la collecte, l'utilisation et l'entreposage de renseignements délicats sur la santé.

Peut-être n'avez-vous pas le choix! Ces dernières années, un certain nombre de lois ont été adoptées pour mieux protéger la vie privée. Ces lois obligent bien souvent les entreprises à rattraper le retard qu'elles accusent dans le domaine de la protection de la vie privée, au risque de devoir payer des amendes salées ou d'être poursuivies en justice.

En octobre 2003, l'État de la Californie a adopté l'Online Privacy Protection Act pour

Additionally, in October of 2003, California passed the Online Privacy Protection Act, reflecting the growing expectation for vigilance in the privacy arena. The Act gives companies only nine months to come into full compliance. By July 2004, every Web site either in California or collecting personal information from California consumers must post a privacy statement online.

The Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada now requires all Canadian industries and organizations to comply with its privacy rules.

Privacy Legislation

Financial service companies must post a privacy statement outlining certain data security measures under the Gramm-Leach-Bliley Act (GLBA).

Children's sites must obtain verifiable parental consent before gathering information from children under the Children's Online Privacy Protection Act (COPPA).

Sites doing business with the European Union are subject to the EU Data Directive, regulating the collection, use and security of personal information regarding EU citizens.

Medical and insurance sites may be required to comply with the Health Insurance Portability and Accountability Act(HIPAA), regulating the collection, use and storage of health-sensitive information.

Posting a privacy statement online is the industry standard. Most Web sites now post an online privacy statement. This trend is in response not only to growing consumer concerns, but also mounting sentiment within the industry that e-businesses were gaining the reputation of being irresponsible data handlers susceptible to hackers and other security breaches. In addition to allaying consumer anxieties, creating and maintaining a privacy policy forces a company to understand its data-handling practices and may reveal potential liabilities that could threaten and undermine its brand.

Creating a privacy policy requires a company to undergo a thorough evaluation of the ways in which it collects, processes, uses, shares, and stores consumer data. This involves taking a comprehensive look at privacy and security, reviewing everything from personnel responsibilities to service provider contacts and from Web encryption to offline data storage. An organization must delve

répondre aux attentes grandissantes relativement à la protection de la vie privée. Cette loi ne donnait que neuf mois aux entreprises pour se conformer. En juillet 2004, tous les sites Web d'entreprises établies en Californie ou recueillant des renseignements auprès de consommateurs californiens devaient afficher un énoncé de protection de la vie privée en ligne.

La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDÉ) du Canada exige maintenant de toutes les industries et organisations canadiennes qu'elles se conforment à ses règles de protection de la vie privée.

L'affichage d'un énoncé de protection de la vie privée en ligne est maintenant devenu la norme dans l'industrie. La plupart des sites Web affichent désormais des énoncés de protection de la vie privée. Cette tendance répond non seulement aux préoccupations grandissantes des consommateurs, mais aussi au sentiment des milieux industriels eux-mêmes qui s'aperçoivent à quel point la réputation des entreprises électroniques souffre de ce qui passe pour leur irresponsabilité face à la menace des pirates informatiques et aux brèches dans la sécurité des données. En plus d'apaiser les craintes des consommateurs, la rédaction et la tenue à jour d'un énoncé de protection de la vie privée obligent les entreprises à étudier leurs pratiques de traitement des données, exercice qui révèle parfois des lacunes susceptibles de présenter un risque pour l'entreprise et de porter atteinte à sa marque de commerce.

Quand elle élabore une politique de protection de la vie privée, l'entreprise doit évaluer en profondeur sa manière de recueillir les données auprès des consommateurs, de les traiter, de les utiliser, de les partager et de les entreposer. Il lui faut donc examiner à fond les problèmes de protection de la vie privée et de sécurité, prendre connaissance de tous les aspects du dossier — des responsabilités de ses employés aux contacts des fournisseurs de services et de l'encodage sur le Web à l'entreposage des données hors ligne. L'entreprise doit vérifier, dans les moindres détails, sa manière de traiter et de partager les renseignements personnels, à l'interne comme à l'externe, pour pouvoir cerner les faiblesses de ses méthodes le cas échéant.

Cette nécessité d'élaborer une politique de

into the details of how personal information is handled and shared both internally and externally to identify potential weaknesses.

The need to create a privacy policy too often occasions a company's first assessment of its data-handling protocol and many companies are surprised to learn that their consumer data is not as well-protected--and its personnel policies not as well-defined--as they may have assumed. Of course, it is always better for a company to uncover any shortcomings on its own rather than having them exposed to the public.

"Privacy isn't just a problem for consumer-oriented business. It affects all businesses, regardless of whether they deal with individual consumers or solely with other enterprises." *Intelligent Enterprise*, 2003

Who Creates a Privacy Statements?

Unless your company is extremely small, chances are good that more than one person will be involved in the creation of your internal privacy policy and, thereafter, your public privacy statement. Members of your management, legal, marketing, operations, and engineering teams may each play a role.

Key Privacy Personnel

Management. The leaders of an organization determine the overall privacy structure and the direction to take.

Legal. Legal experts will ensure that the written policies reflect a company's actual practices.

Marketing. Marketing personnel keep track of a company's current and projected future use of consumer marketing data.

Operations. Those who oversee internal operations can map out and verify a company's workflow and data flow.

Engineering. Information architects know the detailed processes behind a company's transactions and databases.

Sketching out a personal information flow chart is a good way to determine all points of consumer-company contact, to identify which employees

protection de la vie privée est trop souvent la première chance que se donnent les entreprises d'examiner leurs protocoles de traitement des données et il arrive très souvent qu'elles soient surprises, à l'issue de cet exercice, de découvrir que les données de leurs clients ne sont pas aussi bien protégées et leurs politiques relatives au personnel aussi bien définies qu'elles l'avaient pensé. Bien entendu, il est toujours préférable pour une entreprise de découvrir elle-même ses lacunes que d'attendre l'exposition du problème au grand jour.

« La protection de la vie privée ne doit pas intéresser seulement les entreprises qui travaillent auprès des consommateurs. C'est une question qui touche toutes les entreprises, qu'elles traitent avec des particuliers ou d'autres entreprises. » [Traduction] Intelligent Enterprise, 2003

À qui incombe-t-il d'élaborer un énoncé de protection de la vie privée?

Sauf dans le cas des entreprises vraiment très petites, il y a de fortes chances que la tâche d'élaborer la politique interne de protection de la vie privée et, par la suite, l'énoncé correspondant soit confiée à plusieurs personnes. Peuvent aussi intervenir des membres de la direction, des services juridiques, du service de marketing et des équipes des opérations et du génie.

Membres clés de l'équipe chargée de la protection de la vie privée

Direction. Il incombe aux dirigeants de l'organisation de définir l'orientation et la structure générale que prendront les activités de protection de la vie privée.

Services juridiques. Les experts de ces services s'assureront que les politiques adoptées seront conformes aux pratiques réelles de l'organisation.

Service de marketing. Le personnel chargé du marketing se tient au courant des utilisations que l'entreprise fait et compte faire à l'avenir des données de marketing sur les consommateurs.

Opérations. Les responsables du

come into contact with consumer data, how it is shared outside the company, how and where it is stored, and how it is archived or destroyed.

See the figure in Appendix 1

Once there is a general understanding of how data flows through your organization, operations personnel can begin to dig deeper, usually by asking questions of the people involved at each level of the data map.

Questions should be directed to any employees that come into contact with consumer data, including the data engineers who maintain a company's information infrastructure, the communications personnel who seed the customer databases, and the marketing personnel who control use of the information stored in company databases.

Once you have a detailed understanding of how personal information is collected, maintained, and used within your organization, the legal or communications team can step in and draft your privacy statement. At this point the legal team can also make recommendations about how to improve data handling practices if problems are uncovered during the assessment period.

It's extremely important that all the relevant parts of your organization have an opportunity to address privacy issues during the process of creating the privacy policy. If relevant players are left out, not only will the policy be incomplete, it could also end up short of an accurate picture and land your company in legal hot water.

"Privacy requires an integrated approach from both policy and technical perspectives...as a corporate cultural issue, privacy cuts across diverse areas of technology, organization, and regulation." *Cisco Systems*, 2002

What does a Privacy Statement Cover?

At a minimum, a privacy statement should cover the five elements of the Fair Information Practices. This section outlines what types of disclosures are covered under each of the five elements. For best practices, see the following expanded section, "What are Consumer-Friendly Privacy Practices?"

fonctionnement interne de l'entreprise peuvent planifier et vérifier l'ordonnancement des opérations et l'organisation du traitement des données.

Génie. Les architectes de l'information connaissent les méthodes et processus détaillés qui soutiennent les transactions et les bases de données de l'entreprise.

Une bonne façon de trouver tous les points de contact de l'entreprise avec les consommateurs, de déterminer quels employés ont affaire aux données des consommateurs et de savoir comment se fait le partage à l'extérieur de l'organisation, comment se fait l'entreposage et en quel lieu, et comment les données sont archivées ou détruites consiste à dresser un organigramme des opérations de traitement de l'information.

Voir la figure à l'Annexe 1

Une fois qu'on comprend bien l'ordonnancement général des activités de traitement des données dans l'organisation, le personnel chargé des opérations peut approfondir la question, par exemple en s'informant auprès des personnes qui interviennent à chacun des niveaux de l'organigramme.

Il convient de poser des questions à tous ceux qui ont à travailler avec les données sur les consommateurs, y compris les ingénieurs des données qui s'occupent de l'infrastructure de l'information, les employés du service des communications qui alimentent les bases de données sur les clients et le personnel du marketing qui surveille l'utilisation de l'information entreposée dans les bases de données.

Une fois qu'elle comprend bien le détail de la collecte, de la tenue à jour et de l'utilisation des renseignements personnels détenus par l'organisation, l'équipe des services juridiques ou des communications peut faire fond sur tout ce travail pour élaborer un énoncé de protection de la vie privée. À ce stade, l'équipe des services juridiques pourra aussi suggérer des façons d'améliorer les pratiques de traitement des données si l'évaluation a révélé des problèmes.

Il est extrêmement important que tous les services pertinents de l'organisation aient la possibilité de travailler au dossier de la protection de la vie privée pendant ce processus, sans quoi la

Notice.
What information is collected. It may seem obvious that consumers would have full knowledge of what information is collected from them, but this isn't always the case. There are two types of information collection: active and passive. Active collection is the obvious form and involves information that users enter about themselves into Web forms. Usually, this information is for contact (like a name and address), financial (a credit card number), or identification (a password) purposes. There is also information that sites can passively collect without users actually having to enter anything. Passive information collection usually involves the use of tracking technology (like cookies or single-pixel GIFs) that harvests information like IP addresses or surfing behavior.

How information is used. Disclosure of how information is used is as important as what information is collected. In a privacy statement, a Web site should disclose how customer information will be used, including marketing purposes (like cross-selling, list-sharing, joint use), data to third parties, or combining customer data with other data for market research or other purposes.

Choice.
Web sites should provide users with choice regarding the dissemination and use of their personal information and should inform users of the choices available to them. Choice is typically presented in two ways: 'opt-in' and 'opt-out.'

Opt-in mechanisms require users to actively give consent, usually by checking boxes or clicking buttons to signify that they would like to have information shared in a certain way. Opt-out mechanisms, on the other hand, make consent the default setting, and users must actively un-check boxes or click out of certain modes to avoid having information shared.

While some Web sites will automatically include consumers on all of their mailing lists, giving consumers broader ranges of choice establishes and increases trust with Web sites

Access.
Web sites should allow users access to update or correct information they have provided online. If direct consumer access cannot be granted, sites should provide a way for users to request that information be corrected or updated.

politique risque non seulement d'être incomplète, mais pourrait aussi donner une idée inexacte du fonctionnement de l'entreprise et la mettre dans de beaux draps si un problème devait la mener devant les tribunaux.

« La protection de la vie privée exige une approche intégrée des considérations techniques et stratégiques. En outre, sur le plan culturel, la protection de la vie privée met en cause les domaines de la technologie, de l'organisation et de la réglementation. » [Traduction] Cisco Systems, 2002

Que doit couvrir un énoncé de protection de la vie privée?

Un énoncé de protection de la vie privée doit au moins couvrir les cinq éléments qui figurent dans les pratiques équitables de traitement des renseignements de la FTC. Dans cette section sont présentés les types de communications couvertes par chacun des cinq éléments en question. Pour prendre connaissance des pratiques exemplaires dans ce domaine, voir la section suivante intitulée « En quoi consistent les pratiques de protection de la vie privée adaptées aux consommateurs? ».

Avis
L'avis doit indiquer quels renseignements sont recueillis. On pourrait penser que les consommateurs savent quels renseignements sont recueillis à leur sujet, mais ce n'est pas toujours le cas. Il existe deux types de collectes : l'active et la passive. La collecte active est celle qui se fait au grand jour et qui suppose que l'utilisateur entre lui-même les renseignements le concernant dans des formulaires électroniques. En général, ces renseignements sont ses coordonnées (son nom et son adresse), des renseignements financiers (un numéro de carte de crédit) ou des renseignements d'identification (un mot de passe). Il y a aussi les renseignements que les sites Web recueillent de manière passive, sans que les utilisateurs interviennent. La collecte passive de renseignements repose habituellement sur des technologies de pistage (comme les témoins de connexion ou les GIF à un pixel) qui recueillent les renseignements comme les adresses IP ou les habitudes de navigation.

L'avis doit aussi indiquer comment sont utilisés les renseignements. Cet élément d'information est

Security.
Web sites should take security precautions to ensure data integrity. Industry standard is to encrypt all pages asking for Social Security Numbers or credit card data with Secured Socket Layers (SSLs). Most browsers will notify consumers when they are on secured pages.

Redress.
Web sites should have a formal process for managing and addressing consumer concerns. At the very least, contact information must be displayed, so consumers can contact the appropriate employees should privacy issues arise.

What are Consumer-Friendly Privacy Practices?

The most privacy-conscious companies set rigorous standards for themselves in protecting the privacy of their consumers. This section outlines some of the industry's best practices.

Notice.
What information is collected. Although there are many marketing and research benefits to storing robust databases of consumer information, the less information a company collects, the easier it is to limit disclosures, minimize liability, increase security, and establish trust. While consumers may readily disclose whatever information is required to complete their online transactions, they become suspicious of sites that ask for extraneous information.

How information is used. Consumer information should not be used for purposes other than what it was obviously intended. For example, if a mailing address is provided for shipment of a product, the same mailing address should not be used to populate lists for catalogs or solicitations, even if they come from the original company that collected the address. The exception to this standard is if a legal procedure requires the disclosure of consumer information. A disclaimer to this extent, however, should certainly be made public in a privacy statement.

Choice.
Industry surveys show consumers prefer opt-in consent modes for uses of their personal information. Nowadays, more consumers are demanding 'double opt-in' mechanisms to signal consent—usually active check-boxes with a follow-up email

tout aussi important que la nature des renseignements recueillis. Dans son énoncé de protection de la vie privée, le site Web doit indiquer à quelles fins sont destinés les renseignements recueillis sur les clients, y compris les fins commerciales (comme la vente réciproque, le partage des listes de clients et l'utilisation conjointe), les données transmises aux tiers ou la combinaison de données avec d'autres à des fins de recherches et autres.

Choix
Les sites Web doivent fournir aux utilisateurs la possibilité de faire des choix au sujet de la communication et de l'utilisation des renseignements personnels les concernant et les aviser de ces choix. Normalement, ces choix prennent deux formes : l'acceptation et le refus.
L'option de l'acceptation exige des utilisateurs qu'ils donnent activement leur consentement, le plus souvent en cochant une case ou en cliquant sur un bouton, pour indiquer qu'ils acceptent que leurs renseignements personnels soient partagés de la façon indiquée. L'option du refus, par contre, fait du consentement le choix par défaut. Autrement dit, les utilisateurs doivent supprimer le crochet de la case ou cliquer pour sortir de la fonction s'ils ne veulent pas partager leurs renseignements.
Certains sites Web incluent automatiquement tous les consommateurs sur leurs listes d'envoi, mais en leur donnant un plus large éventail de choix. Ils ont ainsi plus de chance de nouer avec eux des relations de confiance.

Accès
Tous les sites Web doivent donner aux utilisateurs la possibilité d'accéder aux renseignements qu'ils ont fournis en ligne pour les mettre à jour ou les corriger. S'il n'est pas possible d'accorder un accès direct aux consommateurs, il faut néanmoins leur offrir un moyen de demander la correction ou la mise à jour de leurs renseignements.

Sécurité
Tous les sites Web doivent s'accompagner de précautions pour protéger l'intégrité des données. Dans l'industrie, la norme est d'encoder toutes les pages qui demandent aux utilisateurs leur numéro d'assurance sociale ou de carte de crédit selon le protocole sécurisé de cryptage (SSL). La plupart des fureteurs avisent les consommateurs lorsqu'ils arrivent sur une page sécurisée.

or pop-up asking if users are certain that they want to share information in a certain way. Particularly in email, acting responsibly can mean the difference in higher response rates and increased trust.

See figures in Appendix 2

Access.
It is required to allow users access to the information they provided with entry of a secure password or other comparable means of identification.

Security.
In addition to encryption of pages collecting sensitive information, the most comprehensive online practices also take into consideration other elements of data security, including personnel access to company databases, and offline data storage. Sites should employ authentication procedures (such as a password) when allowing users access to information they have provided. When making disclosures about security procedures, companies should take care not to disclose too much information to avoid breaches of security.

Redress.
Sites should provide contact information for consumers to communicate their privacy-related concerns. Although email may provide the most efficient means of cataloguing problems, consumers also appreciate when live assistance is available.

Industry best practice is to additionally employ a third-party dispute resolution system to ensure consumers that fair decisions are made and enforced. It's important to many consumers to have an unbiased, outside party weigh both sides of an issue before deciding what course of action should be taken.

Consumer-Friendly Privacy Statements

Consumer-friendly statements are thorough. TRUSTe requires its members to post disclosures of

(1) What personally identifiable information is collected
(2) What personally identifiable information third parties collect through the Web site
(3) What organization collects the information
(4) How the organization uses the information
(5) With whom the organization may share user information

Recours
Les sites Web doivent avoir un processus officiel de gestion des préoccupations des consommateurs. À tout le moins doivent-ils afficher les coordonnées d'une personne-ressource avec qui le consommateur peut communiquer s'il a des inquiétudes au sujet de la protection de ses renseignements personnels.

En quoi consistent les pratiques de protection de la vie privée adaptées aux consommateurs?

Les entreprises particulièrement soucieuses de protéger la vie privée de leurs clients s'imposent des normes rigoureuses dans ce domaine. Dans cette section, on examine certaines des pratiques exemplaires de ces entreprises.

Avis
L'avis doit indiquer quels renseignements sont recueillis. S'il est certainement très utile du point de la recherche et du marketing de monter de solides bases de données sur les consommateurs, moins une entreprise recueillera d'information, plus il sera facile pour elle de limiter les communications, de réduire ses responsabilités, d'accroître la sécurité et d'inspirer confiance à ses clients. Alors que les consommateurs peuvent n'éprouver aucune hésitation à fournir l'information nécessaire à leurs transactions en ligne, ils risquent de se méfier lorsqu'on leur demande des renseignements supplémentaires.

L'avis doit aussi indiquer comment sont utilisés les renseignements. Ceux-ci ne doivent pas servir à d'autres fins que celles prévues au départ. Ainsi, si on demande à un client de fournir son adresse postale pour l'expédition d'un produit, cette même adresse ne doit pas servir à l'envoi de catalogues ou à des sollicitations, même si ces activités sont celles de l'entreprise qui a recueilli les renseignements. La seule exception qui tienne survient dans le cas d'une procédure judiciaire en vertu de laquelle l'entreprise est obligée de communiquer l'information qu'elle détient sur le consommateur. L'entreprise doit préciser dans son énoncé de protection de la vie privée son exonération de responsabilité dans de telles circonstances.

Choix
Les sondages menés par l'industrie indiquent que

(6) What choices are available to users regarding collection, use and distribution of the information
(7) What measures the organization takes to protect the information under its control

For a good example, see www.basspro.com. Basspro does a great job of going through all of these topics and telling consumers, in plain language, how their personal information is used to process orders and who may have access to their information.

Additionally, a thorough privacy statement should cover privacy practices offline as well as online, if those practices pertain to information collected online. For example, if a company uses a shipping company to deliver consumer products, the relationship with the service provider should be disclosed in the privacy statement.

Consumer-friendly statements are accessible. A solid statement isn't worth much if consumers can't easily locate it. Statements should be displayed prominently, especially around areas where consumers are encouraged to share personal information. 1-800-DENTIST makes sure that its privacy statement is accessible directly beneath its form on the home page collecting personal information.

Consumer-friendly statements are easy to understand. Statements can be clear without resorting to 'legalese.' Dynadirect clearly explains what SSLencryption is and shows an image of a navigation bar explaining to consumers how to tell when they are on an encrypted page.

Consumer-friendly statements are neither too short nor too long. Consumers are turned off by lengthy privacy statements but also want to be assured that a site addresses all pertinent topics. Many sites cleverly deal with this challenge by giving consumers the option of reading both short summaries and longer, more detailed explanations. eHealth gives short, bolded summaries of each of its policies, followed by longer explanations that make it easy for consumers to skim as well as explore the company's privacy policies. It also lists additional privacy topics at the bottom of the statement. Some sites, like Bolt, shorten their statement by linking to the longer explanations on an entirely separate page.

Consumer-friendly statements are prioritized.

les consommateurs préfèrent les options d'acceptation aux options de refus pour notifier leurs choix quant à l'utilisation de leurs renseignements personnels. De nos jours, les consommateurs exigent de plus en plus des options d'acceptation doubles pour indiquer leur consentement, c'est-à-dire des cases à cocher qui s'accompagnent d'un courriel de suivi ou d'une fenêtre flash où les consommateurs peuvent confirmer qu'ils sont sûrs de vouloir partager leurs renseignements personnels de la façon précisée. Surtout quand l'entreprise se sert du courrier électronique, un comportement responsable de sa part lui assure un taux de réponse plus important et incite davantage à la confiance.

Voir les figures à l'Annexe 2

Accès
Il importe de donner aux utilisateurs le moyen d'accéder aux renseignements qu'ils ont fournis, par exemple avec un mot de passe sécurisé ou un autre mécanisme semblable d'identification.

Sécurité
En plus d'encoder les pages Web à partir desquelles l'entreprise recueille des renseignements personnels, celle-ci a aussi avantage à prendre en considération d'autres éléments de la sécurité des données, dont l'accès par le personnel à ses bases de données et l'entreposage des données hors ligne. Les sites doivent faire usage des outils d'authentification (comme les mots de passe) quand ils autorisent les utilisateurs à accéder aux renseignements qu'ils ont fournis. Quand elles expliquent leurs procédures de sécurité, les entreprises doivent veiller à ne pas donner trop d'information afin d'éviter les brèches dans la sécurité des données.

Recours
Les sites Web doivent fournir aux consommateurs les coordonnées d'une personne-ressource à qui ceux-ci peuvent communiquer leurs craintes au sujet de la protection de leurs renseignements personnels. Bien que le courriel puisse être la manière la plus efficace de cataloguer les problèmes, les consommateurs apprécient aussi le fait de pouvoir parler directement à quelqu'un.
Une pratique exemplaire consiste à proposer un renvoi à un système de règlement des différends indépendant qui garantit aux consommateurs des décisions équitables. Il est souvent important pour les consommateurs d'avoir un tiers pour faire la

Because statements are consumer-facing, they should list the most relevant information first.

Consumer-friendly statements are updated as needed. Corex clearly signals to its consumers when it has updated its privacy statement. A stagnant statement may indicate to consumers that a company does not regularly review its privacy policies.

Privacy Resources

Privacy Exchange
http://www.privacyexchange.org/
Privacy Exchange compiles a bi-weekly e-newsletter, the Privacy Exchange News Flash, full of new and developing issues in privacy.

Privacy & American Business
http://www.pandab.org
Privacy & American Business researches privacy issues from a business standpoint.

The International Assocation of Privacy Professionals
http://www.privacyassociation.org
The International Association of Privacy Professionals is a network of privacy officers from different industries around the world.

EPIC
http://www.epic.org
The Electronic Privacy Information Center posts legislative and technological updates from the realm of privacy.

TRUSTe
http://www.truste.org
TRUSTe administers a Web privacy seal program and publishes a monthly enewsletter containing privacy event listings, expert discussions on current legislation, and technical tips to keep companies and Web sites up to date.

Sources

[1] Westin, Alan F. "Consumer Privacy Attitudes: A Major Shift since 2000 and Why." Privacy & American Business Newsletter: September 2003, v. 10, no. 6.

[2] According to an August 2003 BizRate.com consumer survey. These figures were consistent

part des choses quand un différend les oppose à une entreprise.

Exemples d'énoncés de protection de la vie privée adaptés aux consommateurs

Les énoncés de protection de la vie privée adaptés aux consommateurs sont détaillés. TRUSTe exige de ses membres qu'ils indiquent :

(1) quels renseignements identifiables ils recueillent;
(2) quels renseignements identifiables des tiers recueillent à partir de leurs sites Web;
(3) quelle organisation recueille les renseignements en question;
(4) quelle utilisation l'organisation fait de ces renseignements;
(5) avec qui l'organisation pourrait partager ces renseignements;
(6) quels sont les choix offerts aux utilisateurs à propos de la collecte, de l'utilisation et de la distribution de leurs renseignements personnels;
(7) quelles mesures l'organisation prend pour protéger les renseignements personnels qui lui sont confiés.

Pour avoir un bon exemple d'énoncé de protection de la vie privée, voir le site de Basspro à l'adresse www.basspro.com (en anglais seulement). Cette entreprise passe en revue chacun des éléments ci-dessus et explique aux consommateurs, dans un langage simple, comment elle utilise les renseignements pour traiter les commandes et qui peut y accéder.

Par ailleurs, en plus des pratiques en ligne, un énoncé de protection de la vie privée doit couvrir les pratiques hors ligne si elles mettent en cause des renseignements obtenus en ligne. Par exemple, si une entreprise a recours à une entreprise de livraison pour livrer ses produits aux consommateurs, elle doit faire état de cette relation avec le livreur dans son énoncé de protection de la vie privée.

Les énoncés adaptés aux consommateurs doivent être facilement accessibles. Peu importe qu'il soit bien conçu, si un énoncé est difficile à voir, il ne sert pas à grand-chose. Il doit être bien en vue, à proximité des sections où les consommateurs sont invités à partager des renseignements personnels. Le service américain 1-800-DENTIST

with a similar survey conducted in January 2003.

Cisco Systems: "Privacy and the Law." 1999-2002.

Cline, Jay. "Does Privacy Pay?" Computerworld: June 17, 2003.

Fogg, B.J.; Kameda, T.; Boyd, J; Marshall, J.; Sethi, R.; Sockol, M,; and Trowbridge, T. (2002). "Stanford-Makovsky Web Credibility Study 2002: Investigating what makes Web Sites Credible Today." A Research Report by the Stanford Persuasive Technology Lab and Makovsky & Company. Stanford University. Available at www.webcredibility.org.

Madsen, Mark. "Making Your Privacy Policy Work." Intelligent Enterprise: June 28, 2002.

Peppers & Rogers Group "Privacy: Beyond Compliance. Responsible Information Stewardship." 2003.

Ponemon, Larry. "Turning Privacy Cost into Privacy Value." Privacy Strategies for Customer-Centric Business. Peppers & Rogers Group: 2002.

dispose son énoncé de protection de la vie privée juste sous son formulaire, sur la page d'accueil de son site à partir de laquelle il recueille les renseignements personnels de ses clients.

Les énoncés adaptés aux consommateurs sont faciles à comprendre. Ils sont clairs et évitent le jargon juridique. L'entreprise Dynadirect explique clairement ce qu'est le protocole d'encodage SSL et montre l'image d'une barre de navigation pour expliquer aux consommateurs comment voir s'ils consultent ou non une page encodée.

Un énoncé adapté aux consommateurs n'est ni trop court ni trop long. Les consommateurs n'aiment généralement pas les énoncés trop longs. Néanmoins, ils tiennent à des énoncés qui traitent de tous les aspects pertinents liés à la sécurité. De nombreuses entreprises ont trouvé un bon moyen de régler ce dilemme en proposant aux visiteurs de leurs sites Web un bref résumé accompagné d'explications plus détaillées et plus longues. eHealth offre un court résumé en caractères gras de chacune de ses politiques, mais y ajoute des explications plus poussées que les consommateurs peuvent lire en diagonale. Le site de l'organisation donne aussi à la fin de l'énoncé une liste d'autres sujets liés à la protection de la vie privée. Certains sites, comme celui de Bolt, proposent des énoncés courts qu'ils complètent par des liens à des explications plus détaillées sur une page distincte.

Par ailleurs, les énoncés adaptés aux consommateurs respectent l'ordre d'importance des sujets qu'ils traitent. Ainsi, ils énumèrent en premier les éléments d'information les plus pertinents pour les consommateurs.

Enfin, les énoncés adaptés aux consommateurs sont mis à jour en fonction des besoins. Corex signale clairement à ses consommateurs les mises à jour de son énoncé. Un énoncé qui stagne donne aux consommateurs l'impression que l'entreprise ne revoit pas souvent ses politiques de protection de la vie privée.

Sites utiles sur la protection de la vie privée *(Veuillez noter que ces sites sont en anglais seulement)*

Privacy Exchange
http://www.privacyexchange.org/
PrivacyExchange produit toutes les deux

semaines un bulletin, le PrivacyExchange NewsFlash, qui traite de toutes sortes de questions nouvelles sur la protection de la vie privée.

Privacy & American Business
http://www.pandab.org
Privacy & American Business étudie le problème de la protection de la vie privée du point de vue des entreprises.

The International Association of Privacy Professionals
http://www.privacyassociation.org
L'International Association of Privacy Professionals est un réseau d'experts de la protection de la vie privée qui œuvrent dans différentes industries du monde entier.

EPIC
http://www.epic.org
L'Electronic Privacy Information Center affiche régulièrement sur son site les dernières nouvelles sur la protection de la vie privée des points de vue législatif et technologique.

TRUSTe
http://www.truste.org
TRUSTe administre un programme de sceaux garants de la sécurité sur le Web et publie un bulletin électronique mensuel qui donne le programme des activités concernant la protection de la vie privée, le détail des débats d'experts sur les lois en cours d'élaboration ou d'adoption, et des conseils technologiques novateurs.

Notes et bibliographie

[1] Westin, Alan F. « Consumer Privacy Attitudes: A Major Shift since 2000 and Why », Privacy & American Business Newsletter, vol. 10, no 6 (septembre 2003).

[2] D'après un sondage réalisé en août 2003 par BizRate.com. Ces chiffres correspondent à ceux d'un autre sondage effectué en janvier 2003.

CISCO SYSTEMS. *Privacy and the Law*, 1999-2002.

CLINE, Jay. « Does Privacy Pay? », *Computerworld*, 17 juin 2003.

FOGG, B.J., T. Kameda, J. Boyd, J. Marshall,

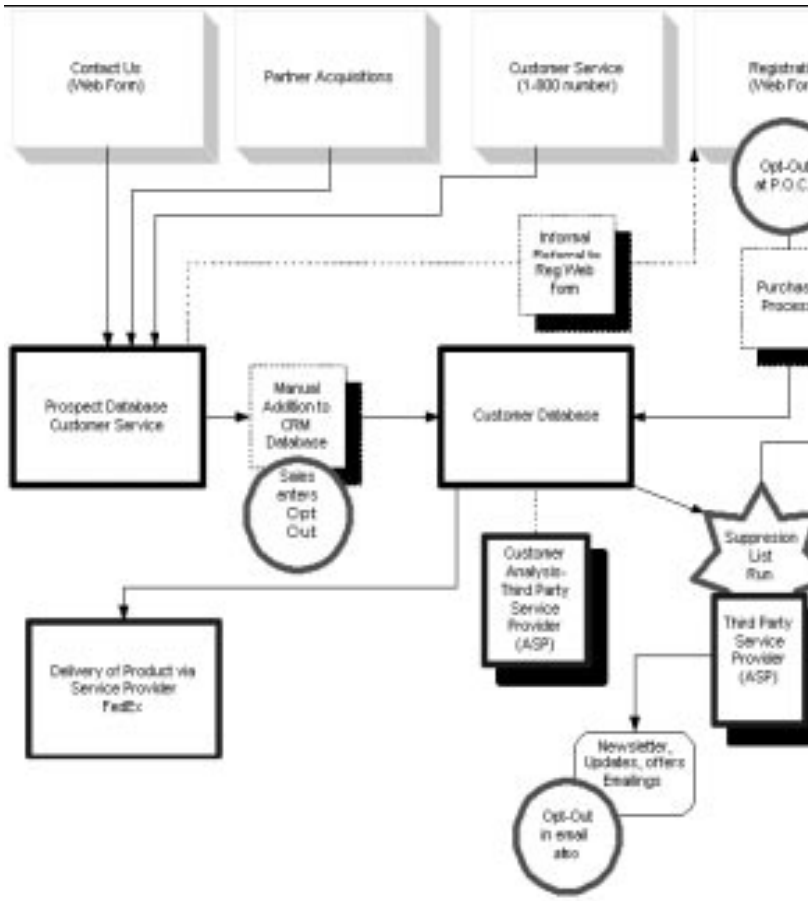
R. Sethi, M. Sockol et T. Townbridge. *Stanford-Makovsky Web Credibility Study 2002: Investigating What Makes Web Sites Credible Today*, Rapport de recherche du Stanford Persuasive Technology Lab et de Makovsky & Company, Stanford University, 2002, www.webcredibility.org.

MADSEN, Mark. « Making Your Privacy Policy Work », *Intelligent Enterprise*, 28 juin 2002.

PEPPERS & ROGERS GROUP. *Privacy: Beyond Compliance. Responsible Information Stewardship*, 2003.

PONEMON, Larry. « Turning Privacy Cost into Privacy Value », *Privacy Strategies for Customer-Centric Business*, Peppers & Rogers Group, 2002.

Annexe 1 / Appendix 1



Dans l'exemple ci-dessus, on voit l'ordonnancement typique des activités de traitement de données pour un site Web de vente au détail. Au haut figurent les divers points de collecte de données auprès des consommateurs par l'entreprise : formulaires électroniques sur le Web, service de dépannage à l'intention des clients et acquisitions des partenaires. L'organigramme montre ensuite à quoi sont destinés les renseignements recueillis, à quels stades les clients peuvent exercer leurs choix et comment ces choix sont pris en considération dans le traitement des données.

This sample map shows the typical flow of data for a retail Web site. At the top level are the company's various collection points for customer data: Web forms, a customer service hotline, and partner acquisitions. The chart then goes on to show for what purposes customer information will be used, at which points a customer is allowed to exercise choices, and how these choices are incorporated into the data.

Annexe 2 / Appendix 2

Exemple d'option d'acceptation. L'utilisateur doit cocher la case du bas pour recevoir un bulletin d'information

An example of an opt-in mode of consent. Users must check the bottom box in order to receive a newsletter.

Exemple d'option de refus. L'utilisateur doit sélectionner le bouton « non » pour éviter de recevoir un courriel

An example of an opt-out mode of consent. Users must fill the 'No' radio button to avoid receiving an email.

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

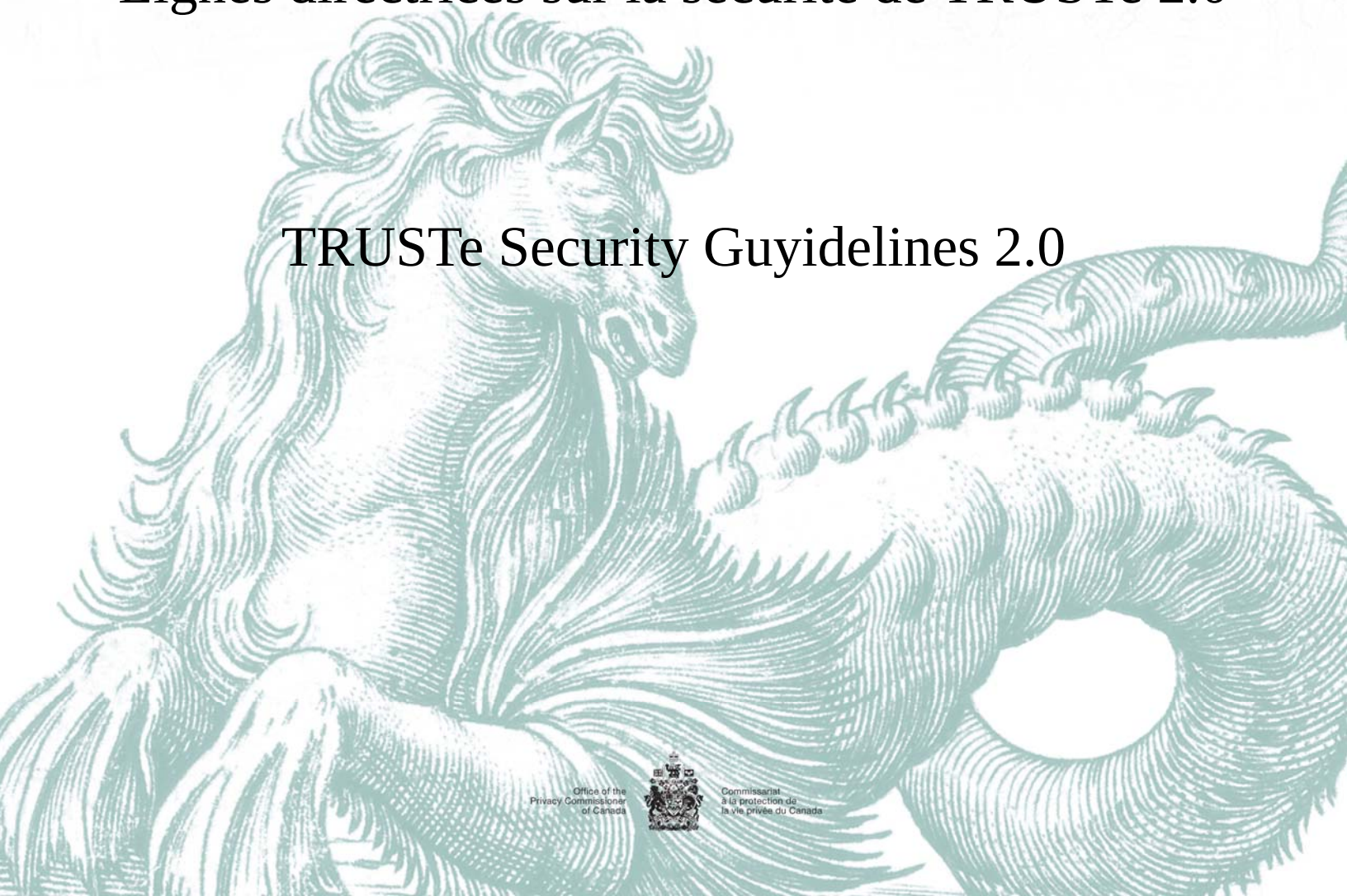
TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Lignes directrices sur la sécurité de TRUSTe 2.0

TRUSTe Security Guyidelines 2.0



Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Résumé

Les activités criminelles de plus en plus fréquentes contre les données sur les clients et les employés minent les efforts pour protéger la vie privée en plus d'ébranler la confiance des intéressés. Nous sommes donc heureux de proposer aux détenteurs de licences TRUSTe et aux autres membres du public des lignes directrices révisées sur la sécurité des données. Les présentes lignes directrices s'inscrivent dans la vaste mission de TRUSTe qui est de faire respecter davantage la confidentialité des renseignements personnels et identitaires. Pour être efficaces, les mesures de protection des renseignements personnels des consommateurs doivent s'appuyer sur des pratiques responsables en matière de sécurité des données.

Cette nouvelle version des lignes directrices renferme des renseignements supplémentaires sur trois domaines importants de la sécurité des données. D'abord, on accorde une plus grande attention à la sécurité des applications Web. Ensuite, on a ajouté des directives sur les appareils mobiles. Enfin, on a consacré deux nouvelles sections à la préparation en vue d'aider les entreprises à mieux faire face à d'éventuelles brèches dans la protection des données.

Les normes de sécurité ne sont pas les mêmes pour tout le monde. Les bonnes normes, commercialement raisonnables, doivent tenir compte de facteurs comme la taille et la complexité de l'entreprise, le type d'industrie, la nature plus ou moins délicate des données recueillies, le nombre de clients desservis et le recours ou non à des fournisseurs de l'extérieur. Dans les présentes lignes directrices, nous avons organisé les mesures de protection selon cinq sections. Les sections 1, 2 et 3 traitent des mesures de protection administratives, techniques et physiques. Les sections 4 et 5 sont essentiellement nouvelles et traitent respectivement des plans d'intervention en cas d'incident et des avis de brèche dans la protection des données. Toutes les pratiques recommandées sont présentées sous forme de liste afin d'aider les entreprises à évaluer leur niveau de risque et à adopter les pratiques qui conviennent le mieux à leur réalité.

Summary

Increasing criminal attacks on consumer and employee data have wrought a high price on individual privacy and trust. In accordance with TRUSTe's broad mission to increase respect for personal identity and information, we are therefore pleased to issue these revised Data Security Guidelines for use as a resource by our licensees and other members of the public. Meaningful protection of consumer privacy depends on a foundation of responsible data security practices.

This new version of the Guidelines provides additional information in three important areas of data security. First, more attention has been given to web application security. Additional guidelines for mobile devices have also been added. Finally, preparation for possible data breaches has been addressed in two new sections.

Security standards are not "one size fits all." Responsible, commercially reasonable standards vary, depending on such factors as a company's size and complexity, industry category, sensitivity of data collected, number of customers served, and use of outside vendors. These Security Guidelines are divided into five categories of safeguards: Parts 1, 2, and 3 address overall administrative, technical, and physical safeguards. Parts 4 and 5 are substantially new sections and address incident response plans and breach notice processes, respectively. All recommended practices are presented in a checklist form so that companies can assess their own risk levels and adopt the practices most appropriate to their particular circumstances.

Introduction

Security Enables Privacy Protection

Meaningful protection of consumer privacy depends on a foundation of responsible data security practices. In accordance with TRUSTe's broad mission to increase respect for personal identity and information, we are therefore pleased to issue Data Security Guidelines for use as a resource by our licensees and other members of the public. We hope these Guidelines will help facilitate internal discussion between privacy and security groups, assist companies as they initially draft their internal security policies, and be useful as a checklist to confirm and perhaps doublecheck existing policies. These practices are not intended

Introduction

La sécurité permet de protéger les renseignements personnels

Les bonnes mesures de protection des renseignements personnels reposent sur des pratiques responsables de sécurité des données. Nous sommes donc heureux de proposer aux détenteurs de licences TRUSTe et aux autres membres du public des lignes directrices révisées sur la sécurité des données. Les présentes lignes directrices s'inscrivent dans la vaste mission de TRUSTe qui est de faire respecter davantage la confidentialité des renseignements personnels et identitaires. Avec elles, nous espérons encourager la discussion entre les groupes responsables des renseignements personnels et de la sécurité, aider les entreprises qui élaborent leur toute première politique interne sur la sécurité, et proposer un outil de vérification qui leur permettra de confirmer l'utilité de leur politique existante. Les pratiques que nous proposons se veulent des outils et non des obligations pour les détenteurs de licences TRUSTe.

La présente version des lignes directrices vient compléter nos pratiques déjà recommandées en matière de sécurité des applications Web, de sécurité des appareils mobiles et des pratiques exemplaires à suivre en cas de brèche dans la protection des données, y compris les avis publics à faire paraître dans ces circonstances.

La sécurité des applications Web traite de la manière de protéger les sites Web contre le piratage. Les applications Web servent à administrer les sites Web dont elles assurent les principales fonctions. Elles incluent des formulaires de collecte de renseignements personnels, classifiés et confidentiels comme sur les antécédents médicaux, le crédit et les comptes bancaires, en plus des commentaires des clients.

Personne, sur Internet, n'est à l'abri du piratage. Dans la course vers la prestation de services en ligne, les entreprises ont souvent élaboré et déployé leurs applications Web sans guère se soucier des risques pour la sécurité. On se retrouve donc avec un nombre étonnant de sites d'entreprises relativement faciles à pirater. Pourtant, les conséquences d'un tel piratage peuvent être désastreuses : perte de revenus, perte de crédibilité, responsabilité légale et perte de confiance des consommateurs. La sécurité des

as mandatory procedures for TRUSTe licensees.

This version of the Guidelines supplements our previously recommended practices in the areas of web application security, mobile device security, and best practices related to data breach incident response, including potential public notification of any such breach.

Web application security focuses on the ways that sites might be vulnerable to hackers. Web applications are used to perform most major tasks or website functions. They include forms that collect personal, classified, and confidential information such as medical history, credit and bank account information and user feedback.

No one on the Internet is immune from security threats. In the race to develop online services, web applications have often been developed and deployed with minimal attention given to security risks, resulting in a surprising number of corporate sites that are vulnerable to hackers. The consequences of a security breach are great: loss of revenues, damage to credibility, legal liability, and loss of customer trust. Web application security is a significant privacy and risk compliance concern and organizations should identify and address web application security vulnerabilities as part of an overall web risk management program.

We have also supplemented recommended safeguards as they relate to mobile devices, particularly those on which sensitive information is stored. While this is not a new area of concern, mobile devices have surfaced as a point of vulnerability for many businesses, as evidenced by a number of publicly-acknowledged breaches traceable to, for example, stolen laptops containing sensitive information. As technology develops, new methods
of transmitting, receiving and storing personal data via mobile devices are created. This poses new problems for privacy protection. The Guidelines set forth some simple steps that can assist companies in determining how to handle data security on mobile devices.

Finally, two sections relating to incident response in general, and specifically breach notices, have been added. Because of the many data breaches recently, many states have now enacted legislation requiring companies to protect data and notify affected individuals. As companies contemplate these legal requirements, as well as a desire to

applications Web constitue donc un élément fondamental de toute stratégie de protection des renseignements personnels et d'atténuation des risques connexes, et les entreprises ont intérêt à cerner et à rectifier les lacunes de leurs applications Web dans le cadre de leur programme général de gestion des risques du Web.

Nous avons aussi proposé des mesures de protection de la sécurité pour les appareils mobiles, en particulier ceux sur lesquels sont entreposés des renseignements de nature délicate. Si ce domaine de préoccupations n'a rien de nouveau, il faut savoir que les appareils mobiles sont bien souvent les éléments vulnérables des stratégies de sécurité des entreprises comme l'ont publiquement démontré des cas d'infractions liés, par exemple, à des appareils portatifs volés qui contenaient des renseignements délicats. À mesure que la technologie évolue, de nouvelles méthodes apparaissent pour transmettre, recevoir et entreposer des renseignements personnels par la voie d'appareils mobiles. Ces méthodes posent de nouveaux problèmes du point de vue de la protection des renseignements personnels. Les présentes lignes directrices proposent quelques mesures simples pour aider les entreprises à protéger les données des appareils mobiles.

Enfin, nous avons ajouté deux sections, une sur les interventions nécessaires en cas de brèche dans la protection des données en général et une autre sur les avis à faire paraître en cas d'infraction. Devant les fréquentes intrusions survenues récemment dans les données des entreprises, bon nombre d'États américains ont adopté des lois qui obligent les entreprises à protéger leurs données et à notifier les personnes dont les renseignements personnels ont fait l'objet d'une intrusion. Quand elles examinent ces obligations légales et pour préserver la confiance que placent en elles leurs clients, les entreprises peuvent s'inspirer des suggestions des présentes lignes directrices sur la manière de se préparer en vue d'une éventuelle brèche dans la protection des données.

Les Lignes directrices en application

Les normes de sécurité ne sont pas les mêmes pour tout le monde. Les bonnes normes, commercialement raisonnables, doivent tenir compte de facteurs comme la taille et la complexité de l'entreprise, le type d'industrie, la

maintain customer trust even in the face of data breaches, these Guidelines set forth some recommended steps to help companies be prepared in the event of a data breach.

Using the Guidelines

Security standards are not "one size fits all." Responsible, commercially reasonable standards vary, depending on such factors as a company's size and complexity, industry category, sensitivity of data collected, number of customers served, and use of outside vendors.

The Security Guidelines are drafted in checklist form so that companies can assess their own risk levels and adopt the corresponding appropriate level of recommended safeguard practices. Larger, more complex companies which handle data with the highest level of sensitivity will likely find it appropriate to adopt all the recommended practices, while a smaller company, collecting less sensitive information, may conclude that adopting only a subset of these controls will still enable it to have a security program appropriate to the nature of the data it collects and handles.

These Security Guidelines are divided into five categories of safeguards: Parts 1, 2, and 3 address overall administrative, technical, and physical safeguards. Parts 4 and 5 address incident response plans and breach notice processes, respectively. Administrative controls include, for example, drafting a written internal security policy, training employees, conducting ongoing security risk assessments, and establishing procedures in connection with external third parties (including vendors) with whom data is shared. Technical measures include controlling employee access to sensitive information on a need-to know basis, establishing good password practices, ongoing monitoring to assess threats and vulnerabilities, ensuring web application security, and establishing incident response procedures. Physical controls include practices such as monitoring legitimate access to data, establishing physical access controls, and securing one's data facilities. Finally, incident planning and response controls include creating a response team, creating a response plan, and formulating a breach notification policy.

Following each of these three main categories, the user will find different types of safeguards, each followed by a number of more detailed supporting directives.

nature plus ou moins délicate des données recueillies, le nombre de clients desservis et le recours ou non à des fournisseurs de l'extérieur.

Les pratiques que nous recommandons sont présentées sous forme de liste afin d'aider les entreprises à évaluer leur niveau de risque et à adopter les pratiques qui conviennent le mieux à leur réalité. Les entreprises plus importantes et plus complexes, qui traitent des données de nature extrêmement délicate, trouveront certainement utile d'adopter toutes les pratiques recommandées, alors que les entreprises de plus petite envergure, qui recueillent des renseignements relativement moins délicats, pourront se contenter d'adopter une portion seulement des pratiques recommandées pour leur programme de sécurité.

Les présentes lignes directrices sont divisées en cinq sections. Les sections 1, 2 et 3 traitent des mesures de protection administratives, techniques et physiques. Les sections 4 et 5 traitent respectivement des plans d'intervention en cas d'incident et des processus de notification des brèches dans la protection des données. Parmi les mesures administratives figurent, par exemple, la rédaction d'une politique interne de la sécurité, la formation des employés, la tenue d'évaluations régulières des risques pour la sécurité et l'adoption des règles à suivre dans les rapports avec des tiers (y compris les fournisseurs) appelés à utiliser les données de l'entreprise. Les mesures techniques sont celles qui, par exemple, permettent de limiter l'accès des renseignements délicats aux seuls employés qui en ont besoin pour leur travail, de gérer l'accès par mot de passe, de surveiller continuellement les systèmes pour repérer les menaces et cerner les faiblesses, de protéger les applications Web et d'établir la marche à suivre en cas de brèches dans la protection des données. Les mesures physiques comprennent la surveillance de l'accès légitime aux données, la prise de mesures de surveillance physiques et la protection des installations où sont entreposées les données. Enfin, par planification des interventions en cas d'incident et des mesures connexes, on entend la création d'une équipe d'urgence, l'élaboration d'un plan d'intervention et la formulation d'une politique de communication des brèches dans la protection des données.

Dans chacune des trois sections principales, l'utilisateur trouvera différents types de mesures

For the user's convenience, the Guidelines are presented in checklist form, with each recommended control accompanied by checkboxes which the user can fill in with his or her own assessment of whether the practice is appropriate and relevant to the user's particular company, as follows:

Should be required – A check in this category means that you believe the practice or procedure should be implemented within your organization to achieve reasonable data protection levels.

Should be optional – A check in this category means that you believe the practice or procedure will be useful, but may not be appropriate within your organization to achieve reasonable data protection levels.

Not relevant – A check in this category means that you believe the practice or procedure will not be useful within your organization for purposes of data protection.

Guiding Principles

We recognize that companies may achieve reasonable security through other measures, not included within the Guidelines. While the Guidelines rely upon other learned information security standards such as ISO 17799 and the Payment Card Industry (PCI) Guidelines, and are informed by regulatory requirements such as those imposed by the Gramm Leach Bliley Act and HIPAA, they are not intended as a comprehensive list of all leading security measures. Rather, the
Guidelines are intended to provide a relatively non-technical, high level overview of responsible security practices. For those users wishing a more detailed or technological focus, the Guidelines also contain links to an array of information security websites which some users will find helpful.

We anticipate that the Guidelines will evolve over time to reflect emerging technologies and business issues that may impact the safety, security and quality of sensitive or confidential information used by TRUSTe's licensees. Finally, we welcome suggestions and comments via email to policylegal@truste.org.

Sources

Following are the main sources used to draft the attached Guidelines:

de protection, chacune accompagnée d'un certain nombre de directives plus détaillées.

Pour faciliter le travail de l'utilisateur, nous avons présenté nos directives sous forme de liste avec des cases que l'utilisateur peut cocher s'il estime la directive utile et applicable à son entreprise.

Directive fondamentale. Un crochet dans cette catégorie de directives indique que vous jugez la pratique ou la méthode proposée indispensable à votre organisation si elle veut protéger correctement ses données.

Directive facultative. Un crochet dans cette catégorie indique que vous jugez la pratique ou méthode proposée utile, mais qu'elle ne convient peut-être pas à votre organisation dans ses efforts pour protéger correctement ses données.

Directive inutile. Un crochet dans cette catégorie indique que vous jugez la pratique ou méthode proposée inutile pour la protection des données de votre organisation.

Principes directeurs

Il est clair qu'il existe certainement d'autres moyens que ceux que nous proposons de protéger les données des entreprises. Nos recommandations s'inspirent toutefois de normes de sécurité de l'information reconnues, comme la norme ISO 17799 et les directives de l'industrie des paiements par carte, en plus de prendre appui sur les exigences de la *Gramm Leach Bliley Act* et de la *Health Insurance Portability and Accountability Act*. Cela dit, nous n'avons pas la prétention d'énumérer de façon exhaustive toutes les mesures de sécurité de pointe. Nous avons plutôt essayé de donner un aperçu pas trop technique et assez général des pratiques nécessaires à une protection raisonnable de la sécurité. Pour les utilisateurs à la recherche d'informations plus détaillées ou plus techniques, nous proposons des liens vers une série de sites Web sur la sécurité de l'information.
Nous prévoyons mettre à jour nos lignes directrices en fonction de l'évolution de la technologie et d'autres facteurs qui pourraient influer sur le contexte de la sécurité et la protection des renseignements délicats et confidentiels qu'utilisent les détenteurs de licences TRUSTe. Nous vous invitons à nous faire parvenir par courriel vos suggestions et

International Organization for Standardization (ISO) 17799. ISO-17799 is an International recognized Information Security Management Standard first published in December 2000, derived from British Standard 7799 Parts I and II.

Visa USA Cardholder Information Security Program (CISP). Established in June 2001, the program is intended to protect Visa cardholder data to ensure that members, merchants, and service providers maintain reasonably high information security standard. In addition to the CISP "digital dozen," we included new features from the PCI Data Security Guidelines.

Organisation for Economic Co-Operation and Development (OECD), Guidelines for the Security of Information Systems. In addition, we reviewed various papers published by the Business and Industry Advisory Committee (BIAC) to the OECD.

Acknowledgments

TRUSTe would like to acknowledge the many experts we consulted in revising these Guidelines.

Dr. Larry Ponemon of the Ponemon Institute was instrumental in developing these Guidelines. Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government.
www.ponemon.org

Watchfire provided input and guidance in developing the Web application security guidelines. Watchfire is a provider of Online Risk Management software and services to monitor and report online security, privacy, quality, accessibility, and compliance risks. For more information on Watchfire and its web application security expertise please visit:
http://www.watchfire.com/securityzone/default.aspx

Joanne McNabb, Chief, California Office of Privacy Protection, provided guidance in connection with the new incident response sections. The California Office of Privacy Protection assists individuals with identity theft and other privacy-related concerns; provides consumer education and information on privacy issues; coordinates with local, state and federal law enforcement on identity theft investigations; and recommends policies and practices that protect individual privacy rights.

commentaires à l'adresse policylegal@truste.org.

Sources

Les sources ci-dessous sont les principales dont nous nous sommes servis pour élaborer nos lignes directrices :

Norme ISO 17799 de l'Organisation internationale de normalisation. La norme ISO-17799 est une norme internationale reconnue de gestion de la sécurité de l'information. Publiée pour la première fois en décembre 2000, elle est inspirée d'une norme britannique, la norme 7799, parties I et II.

Le programme de protection des renseignements sur les détenteurs de cartes (Cardholder Information Security Program ou CISP) de Visa USA. Créé en juin 2001, ce programme a pour but de protéger les détenteurs de cartes Visa en leur garantissant que les membres, les marchands et les fournisseurs de services du réseau Visa observent des normes raisonnablement élevées de sécurité de l'information. En plus de la « douzaine numérique » du CISP, nous avons emprunté des ajouts aux Lignes directrices sur la sécurité des données du PCI.

Organisation de coopération et de développement économiques (OCDE), Lignes directrices régissant la sécurité des systèmes et réseaux d'information. En outre, nous avons examiné de nombreux rapports publiés par le Comité consultatif économique et industriel (BIAC) auprès de l'OCDE.

Remerciements

TRUSTe aimerait remercier les nombreux experts que nous avons consultés à l'occasion de la révision des présentes lignes directrices.

M. Larry Ponemon, du Ponemon Institute, a largement contribué à l'élaboration des lignes directrices. Le Ponemon Institute réalise des travaux de recherche indépendants et offre des services de formation sur les pratiques responsables de gestion de l'information et de protection de la vie privée au profit des entreprises et des organismes publics.
www.ponemon.org

www.privacy.ca.gov

TRUSTe would also like to recognize the contributions of Ernst & Young and ChoicePoint Inc.

See Appendix

Data Categories

When establishing security controls, it is useful to categorize data by level of sensitivity.
These are some possible data categories:

Sensitive Personal Data
Data that is (1) identifiable to an individual person and (2) has the potential to be used to harm or embarrass the data subject.

- Social Security Numbers
- National ID Numbers
- Driver's license number
- Credit Card numbers
- Account numbers
- Passwords, including PINs*
- Criminal arrests or convictions
- Judgments in civil cases
- Medical information
- Administrative sanctions
- Race, ethnicity, national origin
- Data concerning sexual orientation or activity
- Financial data (such as credit rating)
- Salary & compensation
- Disability status

Ordinary Personal Data
Data that is identifiable to an individual person but that is generally considered to have a lower level of sensitivity than "Sensitive Data".

- Name
- Telephone # (work & home)
- Address (work & home)
- Email address (work and home)
- Gender
- Marital status
- Number of children
- Date of birth or age
- Citizenship
- Education
- Income range
- Non-medical benefits information
- Purchase history
- Buying patterns
- Hobbies and interests

La société Watchfire a aussi commenté et guidé l'élaboration des lignes directrices. Fournisseur de logiciels et de services de gestion du risque en ligne, Watchfire donne à ses clients les moyens de surveiller les risques auxquels ils s'exposent en ligne sur les plans de la sécurité, de la protection de la vie privée, de la qualité, de l'accessibilité et de la conformité, et de produire des rapports de conformité. Pour plus d'information sur Watchfire et son travail en sécurité des applications Web, veuillez visiter le site http://www.watchfire.com/securityzone/default.aspx

Joanne McNabb, directrice du Commissariat à la protection de la vie privée de la Californie, nous a donné de précieux conseils pour les sections sur les interventions en cas d'incident. Le Commissariat aide les citoyens de l'État aux prises avec des problèmes de vols d'identité et de non-respect de leur vie privée; organise des activités d'information sur la protection de la vie privée en plus de diffuser de l'information à ce sujet auprès des consommateurs; coordonne les activités d'application de la loi avec les administrations locale, étatique et fédérale lors d'enquêtes sur des vols d'identité; et recommande des pratiques et des politiques qui protègent le droit des personnes à la vie privée.
www.privacy.ca.gov

TRUSTe souhaite aussi souligner les contributions d'Ernst & Young et de ChoicePoint Inc.

Voir l'annexe

Catégories de données

Au moment d'établir les contrôles de sécurité, il est bon de regrouper les données selon leur caractère névralgique.

Voici des exemples de catégories :

Données personnelles délicates
Données qui permettent 1) d'identifier la personne à qui appartiennent les données et qui 2) pourraient être utilisées pour nuire à cette personne ou la mettre dans l'embarras.

Numéros de sécurité sociale
numéro d'identité national
numéro de permis de conduire
numéros de carte de crédit
numéros de compte

Information Security Sites

Introductory
http://www.iccwbo.org/home/e_business/securing_your_business.pdf

http://www.biac.org/statements/iccp/Final_Information_Security_for_Executives071003.pdf

http://www.ftc.gov/infosecurity/

http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase

http://www.sans.org/top20/

General
http://www.infosyssec.net/
http://www.cerias.purdue.edu/

Technical / Alerts / Advisories
http://www.cert.org/
http://www.cisecurity.org/
http://www.ciac.org/ciac/index.html

Magazines / Publications
http://www.csoonline.com/
http://informationsecurity.techtarget.com/
http://www.scmagazine.com/home/index.cfm
http://www.gsnmagazine.com/

AntiVirus / Malware– current alerts
http://www.trendmicro.com/vinfo/
http://www3.ca.com/securityadvisor/virusinfo/default.aspx
http://www.symantec.com/avcenter/vinfodb.html#threat_list

Certification
http://www.icsalabs.com/index.shtml

ID Theft
http://www.consumer.gov/idtheft/

Crime / Government
http://www.htcia.org/
http://www.infragard.net/

Standards
http://www.nist.gov/
http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html

Incident Response/Breach Notice Sites
http://www.privacy.ca.gov/recommendations/secbreach.pdf

mots de passe, y compris des NIP*
renseignements sur des arrestations au criminel ou des condamnations
décisions d'un tribunal civil
renseignements médicaux
renseignements sur des sanctions administratives
race, ethnie, origine nationale
orientation ou activité sexuelle
renseignements financiers (comme les évaluations de crédit)
renseignements sur la rémunération
renseignement sur une invalidité.

Données personnelles ordinaires
Données qui permettent d'identifier la personne à qui appartiennent ces données, mais qu'on juge généralement moins compromettantes que les données de la catégorie « délicate ».

Nom
numéro de téléphone (à la maison et au travail)
adresse (à la maison et au travail)
adresse courriel (à la maison et au travail)
renseignements sur le sexe
état civil, nombre d'enfants
date de naissance
âge
citoyenneté
niveau d'études
échelle salariale
avantages sociaux non médicaux
achats récents
habitudes d'achat
loisirs et intérêts.

Sites consacrés à la sécurité de l'information

Introduction
http://www.iccwbo.org/home/e_business/securing_your_business.pdf

http://www.biac.org/statements/iccp/Final_Information_Security_for_Executives071003.pdf

http://www.ftc.gov/infosecurity/

http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase

http://www.sans.org/top20/

http://www.cert.org/csirts/csirt_faq.html
http://www.ncsl.org/programs/lis/CIP/priv/breach.htm.

About TRUSTe

TRUSTe, the online privacy leader, is an independent, nonprofit organization dedicated to enabling individuals and organizations to establish trusting relationships based on respect for personal identity and information in the evolving networked world. TRUSTe operates the world's largest Web site privacy seal program providing standards and dispute resolution for more than 1,300 Web sites.

Since 1997,TRUSTe has conducted more than 7,000 Web site privacy policy certifications. Informed by extensive consumer attitude research, TRUSTe provides industry with pragmatic and respectful policy guidance for Web site practices, wireless privacy, email privacy and data security. For more information, visit www.truste.org.

Généralités
http://www.infosyssec.net/
http://www.cerias.purdue.edu/

Sites techniques / Alertes / Avis
http://www.cert.org/
http://www.cisecurity.org/
http://www.ciac.org/ciac/index.html

Magazines/ Publications
http://www.csoonline.com/
http://informationsecurity.techtarget.com/
http://www.scmagazine.com/home/index.cfm
http://www.gsnmagazine.com/

Anti-virus / Logiciels malveillants – avertissements
http://www.trendmicro.com/vinfo/
http://www3.ca.com/securityadvisor/virusinfo/default.aspx
http://www.symantec.com/avcenter/vinfodb.html#threat_list

Accréditation
http://www.icsalabs.com/index.shtml

Vol d'identité
http://www.consumer.gov/idtheft/

Criminalité / Gouvernement
http://www.htcia.org/
http://www.infragard.net/

Normes
http://www.nist.gov/
http://www.iso.org/iso/fr/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm

Interventions en cas d'incident/Avis de brèche dans la protection des données
http://www.privacy.ca.gov/recommendations/secbreach.pdf
http://www.cert.org/csirts/csirt_faq.html
http://www.ncsl.org/programs/lis/CIP/priv/breach.htm

TRUSTe

Chef de file de la protection de la vie privée en ligne, TRUSTe est un organisme indépendant, sans but lucratif, qui vient en aide aux entreprises et aux particuliers soucieux de bâtir des relations de confiance, fondées sur le respect de l'identité et des renseignements personnels dans le monde de plus en plus réseauté d'aujourd'hui. TRUSTe administre le programme de sceau de protection

de la vie privée sur Internet le plus important au monde. Ce programme établit des normes et propose un mécanisme de règlement des litiges pour plus de 1 300 sites Web.

Depuis 1997, TRUSTe a accordé plus de 7 000 accréditations à des sites Web respectueux des règles de protection de la vie privée. Prenant appui sur de solides recherches au sujet des attitudes des consommateurs, TRUSTe offre à l'industrie des conseils stratégiques pratiques et respectueux sur les façons de gérer les sites Web, les communications sans fil, le courriel et les données sous l'angle de la sécurité et de la protection de la vie privée. Pour plus d'information sur TRUSTe, visitez son site Web à l'adresse www.truste.org.

Annexe

Partie 1 : Mesures administratives

1.0	Créer un comité sur la sécurité.	Directive fondamentale	Directive facultative	Directive inutile
1.1	Pour former le comité, réunir une équipe interfonctionnelle qui comptera des représentants des différentes sections de l'organisation.			
1.2	Élaborer la charte du comité sur la sécurité.			
1.3	Désigner, parmi les membres de la haute direction, un champion de la sécurité. Ce dernier devrait également être membre du comité.			

2.0	Élaborer une politique écrite officielle sur la sécurité et adopter un fonctionnement normalisé.	Directive fondamentale	Directive facultative	Directive inutile
2.1	S'assurer que la politique s'applique à toute l'organisation ou qu'il existe des politiques qui visent adéquatement toutes les activités de l'organisation. Veiller en outre à ce que ces politiques cadrent bien avec les autres politiques de l'organisation. Des politiques doivent aussi régir le fonctionnement des sites Web internes et externes.			
2.2	Aligner les politiques sur les autres politiques de contrôle de la conformité, surtout celles qui régissent les relations avec les fournisseurs appelés à utiliser les renseignements personnels et protégés détenus par l'organisation. Avant d'élaborer les politiques, revoir les obligations réglementaires qui se rapportent aux données et aux clients.			
2.3	Veiller à la coordination des différentes versions de la politique sur la sécurité et garder la mainmise sur ces versions.			
2.4	Revoir périodiquement la politique sur la sécurité et le fonctionnement normalisé, et les modifier au besoin en fonction de l'évolution des activités de l'organisation, de la technologie et des circonstances.			
2.5	Faire circuler la politique sur la sécurité et le fonctionnement normalisé dans tous les services pertinents de l'organisation. Prévoir au besoin une version de la politique pour le public ou les intervenants externes, y compris les agents contractuels.			
2.6	Au moyen d'un lien sur chaque page, fournir aux utilisateurs du site Web des renseignements appropriés sur la manière de transmettre de l'information. Penser à ajouter un résumé de la déclaration de l'organisation sur la protection des renseignements personnels et de la vie privée.			

3.0	Effectuer régulièrement des évaluations des risques pour la sécurité.	Directive fondamentale	Directive facultative	Directive inutile
3.1	Trouver les menaces et les faiblesses des systèmes qui présentent des risques pour la sécurité et les classer par ordre de priorité. Examiner au moins les risques dans les domaines suivants : formation et gestion des employés; systèmes d'information; et prévention, détection et intervention dans le cas d'attaques des systèmes ou autres défaillances.			
3.2	Établir un budget des ressources et des dépenses en fonction des risques et de leur gravité relative.			
3.3	Revoir régulièrement les évaluations des risques et les modifier au besoin, à la lumière des changements survenus dans le contexte commercial, technologique et environnemental.			

4.0	Mettre en place un plan de protection de tous les systèmes et réseaux importants.	Directive fondamentale	Directive facultative	Directive inutile
4.1	Revoir régulièrement les plans de protection des systèmes et les modifier au besoin.			
4.2	S'assurer que les plans et les politiques de sécurité prévoient l'examen et la surveillance périodiques des appareils aux extrémités comme les ordinateurs personnels, les ordinateurs portatifs, les assistants numériques et autres appareils branchés à des réseaux ou des systèmes qui traitent des renseignements délicats (y compris les systèmes Bluetooth).			
4.3	Exiger la conclusion d'ententes d'interconnexion entre les systèmes.			
4.4	Exiger la conclusion d'ententes sur l'accès aux systèmes.			
4.5	Procéder à des vérifications périodiques des ententes d'interconnexion et les modifier au besoin.			

5.0	Préparer des plans de secours qui prévoient entre autres la mise à jour des contrôles d'accès.	Directive fondamentale	Directive facultative	Directive inutile
5.1	Préparer des plans de poursuite des activités.			
5.2	Préparer des plans de reprise après sinistre.			
5.3	Préparer des plans d'urgence pour le personnel.			
5.4	Revoir et tester régulièrement les plans de secours, et les modifier au besoin.			

6.0	Intégrer la sécurité dans l'ensemble du cycle de vie des systèmes. Cela signifie entre autres :	Directive fondamentale	Directive facultative	Directive inutile
6.1	Définir les exigences.			
6.2	Établir des méthodes à suivre pour la conception et les achats.			
6.3	Établir des méthodes à suivre pour les tests et l'entretien.			

7.0	Créer un système structuré de sauvegarde des données.	Directive fondamentale	Directive facultative	Directive inutile
7.1	Vérifier que les sauvegardes des données comprennent la mise à jour des contrôles d'accès.			
7.2	Revoir et tester régulièrement les systèmes de sauvegarde des données, et les modifier au besoin.			

8.0	Créer un système de vérification de la sécurité.	Directive fondamentale	Directive facultative	Directive inutile
8.1	Soumettre régulièrement tous les contrôles de sécurité à des vérifications internes et externes. Inclure à la vérification les applications Web ainsi que les hôtes, le réseau et les comptes des utilisateurs.			
8.2	Organiser des exercices de simulation afin de tester la capacité de l'organisation de réagir aux menaces (y compris la vulnérabilité à l'ingénierie sociale).			

9.0	Documenter toutes les configurations des systèmes et des réseaux.	Directive fondamentale	Directive facultative	Directive inutile
9.1	Créer un système structuré de contrôle des configurations et des changements (qui vise aussi les vulnérabilités et leurs corrections), accompagné d'essais de préproduction.			
9.2	Documenter et classer tous les renseignements de nature délicate (inventaire des données).			
9.3	Documenter les règles officielles de comportement, les conditions d'utilisation et les accords de confidentialité pour tout le personnel ayant accès aux renseignements de nature délicate que détient ou traite l'organisation.			
9.4	Documenter la séparation appropriée des fonctions (p. ex., l'administrateur du système ne doit pas être aussi l'administrateur de la sécurité).			
9.5	Documenter les méthodes courantes et d'urgence de suspension de l'accès.			
9.6	Documenter la capacité officielle d'intervention en cas d'urgence.			

10.0	Lancer un programme de sensibilisation et de formation pour les employés.	Directive fondamentale	Directive facultative	Directive inutile
10.1	Créer un mécanisme d'accréditation ou d'autorisation pour les employés qui ont accès aux systèmes importants.			
10.2	Exiger de tous les employés qu'ils suivent une formation introductive et d'appoint. Suivre et documenter la formation suivie par chacun.			
10.3	Encourager la formation et le perfectionnement continus des spécialistes de la sécurité.			

11.0	Définir les méthodes à suivre pour les activités de gestion des données ou de TI confiées à l'extérieur.	Directive fondamentale	Directive facultative	Directive inutile
11.1	Procéder à un contrôle des fournisseurs avant de leur transmettre des renseignements délicats ou confidentiels, y compris des données permettant d'identifier les consommateurs ou les employés.			
11.2	Vérifier les installations du centre de données du fournisseur afin de s'assurer que l'infrastructure de sécurité convient.			
11.3	Obtenir du fournisseur une garantie de sa conformité aux lois et politiques applicables de protection des données et des renseignements personnels des clients.			
11.4	Prévoir dans le contrat un contrôle de l'utilisation des données par le fournisseur et de ses pratiques connexes.			
11.5	Procéder à des vérifications périodiques et aléatoires des activités des fournisseurs.			
11.6	Dans la mesure du possible, vérifier la capacité et la compétence des principaux employés du fournisseur (surtout ceux qui sont chargés de traiter ou de gérer des renseignements personnels délicats).			

Partie 2 : Sécurité technique

1.0	Surveiller l'accès à l'information contenue dans les supports de données comme les serveurs, les ordinateurs personnels, les ordinateurs portatifs et les assistants numériques.	Directive fondamentale	Directive facultative	Directive inutile
1.1	S'assurer que les utilisateurs des systèmes ont chacun leur propre identification ou nom d'utilisateur. Vérifier qu'ils n'utilisent pas leur numéro d'assurance sociale ou de compte comme identification ou nom d'utilisateur.			
1.2	Utiliser des mécanismes d'authentification comme des mots de passe, des jetons ou des éléments biométriques.			
1.3	Exiger des administrateurs des systèmes qu'ils utilisent leurs comptes d'utilisateur réguliers pour tout travail qui n'exige pas d'accéder à l'ensemble du réseau ou à l'administration de la sécurité du système.			
1.4	Accorder les droits d'accès en fonction du besoin de savoir (le droit d'accès doit être fonction des tâches à remplir et non établi d'après le titre ou le niveau dans l'organisation).			
1.5	Dans la mesure du possible, utiliser un mécanisme d'authentification à deux facteurs avant d'accorder aux utilisateurs l'accès à des renseignements délicats.			
1.6	Dans la mesure du possible, adopter une méthode pour traiter les demandes soumises en ligne de changement de nom d'utilisateur et de mot de passe .			
1.7	En cas d'inactivité, imposer une déconnexion automatique, par exemple au bout de 15 minutes ou moins.			

2.0	Adopter une politique régissant l'utilisation des mots de passe qui contiendra les éléments suivants :	Directive fondamentale	Directive facultative	Directive inutile
2.1	Autant que possible, exiger au moins six caractères alphanumériques pour les mots de passe. Demander aux utilisateurs de changer régulièrement leurs mots de passe.			

2.2	Interdire les mots de passe inspirés de numéros de compte, de noms d'utilisateurs, de noms propres, de numéros d'assurance sociale ou de renseignements personnels faciles à deviner (comme les dates d'anniversaire, les noms d'enfants ou d'animaux domestiques, etc.).			
2.3	Décourager la réutilisation des mots de passe.			
2.4	Créer un système d'authentification officiel de l'utilisateur qui réinitialise les mots de passe. Si possible, offrir la possibilité de changer un mot de passe ou de le réinitialiser à partir de la page de connexion. Permettre aux utilisateurs de mettre à jour les questions ou indices de rappel du mot de passe.			
2.5	Au moment d'envoyer la confirmation d'une inscription ou un autre type de message de bienvenue, ne fournir que le nom d'utilisateur dans le courriel et prévoir sur le site Web un dispositif de réinitialisation du mot de passe.			
2.6	Ne pas envoyer dans un même courriel le mot de passe et le nom d'utilisateur ensemble.			
2.7	Prévoir l'expiration des mots de passe.			
2.8	Prévoir la marche à suivre en cas de perte ou de vol d'un ordinateur portatif, y compris l'annulation des mots de passe.			

3.0	Surveiller l'accès à l'information qui peut être affichée, imprimée ou téléchargée sur un appareil de stockage externe, en particulier un ordinateur personnel, un ordinateur portatif ou un assistant numérique.	Directive fondamentale	Directive facultative	Directive inutile
3.1	Prévoir des contrôles d'exploitation qui restreignent les téléchargements de renseignements de nature délicate sans une identification appropriée. (Voir l'annexe pour la classification des données délicates.)			
3.2	Installer des économiseurs d'écran et des écrans de protection pour réduire le risque d'afficher des renseignements délicats à la vue d'utilisateurs non autorisés.			
3.3	Installer des commandes pour mettre à l'arrêt les ordinateurs inactifs.			
3.4	Autant que possible, limiter à la consultation les droits d'accès des utilisateurs d'ordinateurs éloignés ou d'appareils sans fil qui veulent se brancher aux réseaux ou systèmes de l'organisation.			
3.5	Autant que possible, limiter l'utilisation de renseignements personnels sur des ordinateurs portatifs. Si cette utilisation est indispensable, s'assurer que les données sont encodées ou, au moins, que les ordinateurs portatifs sont protégés par des moyens plus sûrs qu'un simple mot de passe.			
3.6	Prévoir des rappels pour que les utilisateurs nettoient périodiquement leurs disques afin d'éliminer les sauvegardes temporaires et vident les poubelles ou le recyclage. Documenter au besoin cette pratique dans les plans de conservation et d'élimination des documents de l'organisation.			

4.0	Surveiller les comptes d'utilisateurs pour repérer et éliminer les utilisateurs inactifs, et plus précisément :	Directive fondamentale	Directive facultative	Directive inutile
4.1	Fermer automatiquement les comptes inactifs depuis 60 jours ou plus.			
4.2	Fermer dans les 24 heures les comptes d'employés mis à pied ou d'entrepreneurs qui ne travaillent plus pour l'organisation.			
4.3	Vérifier régulièrement les comptes d'utilisateurs en fonction des dossiers des RH pour s'assurer que l'accès des anciens employés a bien été fermé.			

5.0	Prévoir des mesures suffisantes pour protéger la transmission et l'entreposage des données, notamment :	Directive fondamentale	Directive facultative	Directive inutile
5.1	Utiliser des méthodes d'encodage raisonnables pour transmettre ou recevoir des renseignements de nature délicate, surtout lorsque l'envoi se fait par le réseau public d'Internet. Employer un code d'encryptage d'au moins 128 bits.			
5.2	Utiliser un protocole WEP (Wireless Encryption Protocol) pour la transmission ou la réception de renseignements délicats d'assistants numériques, de téléphones Web, d'ordinateurs portatifs et d'appareils nouveaux comme ceux qui utilisent les technologies de connexion Bluetooth.			
5.3	Utiliser des méthodes d'encodage raisonnables pour l'entreposage, surtout celui de renseignements délicats sur des serveurs, des ordinateurs personnels et des ordinateurs portatifs.			
5.4	Utiliser des logiciels de réseaux privés virtuels (VPN) pour autoriser et encoder les transmissions d'appareils autorisés, et s'assurer que l'accès VPN est assujetti à des contrôles suffisants et fait l'objet d'une surveillance.			
5.5	Utiliser des outils de vérification de la configuration pour signaler les appareils d'entreposage retirés du réseau ou du système de l'organisation.			
5.6	Restreindre le téléchargement de renseignements personnels délicats d'appareils d'entreposage centraux sur des ordinateurs personnels ou des appareils d'entreposage sans fil.			

6.0	Configurer tous les serveurs, ordinateurs personnels et ordinateurs portatifs avant de les utiliser, notamment :	Directive fondamentale	Directive facultative	Directive inutile
6.1	Désactiver les ports inutilisés.			
6.2	Installer ou activer les dispositifs de verrouillage automatique d'écran afin d'empêcher l'accès après une période définie d'inactivité.			
6.3	Changer tous les mots de passe fournis par défaut par le fournisseur.			
6.4	S'assurer que le protocole WEP (Wireless Encryption Protocol) est activé avant de permettre le branchement d'un appareil sans fil aux systèmes ou réseaux de l'organisation.			
6.5	Traiter toutes les connexions sans fil internes comme des connexions externes.			
6.6	Vérifier régulièrement la capacité d'accès externe non autorisé, y compris à partir des points d'accès sans fil.			
6.7	S'assurer que les installations et configurations logicielles par défaut conviennent, compte tenu des besoins de sécurité, et changer, le cas échéant, les mots de passe ou ajuster les paramètres de sécurité.			

7.0	Configurer les pare-feu pour assurer une protection maximale de l'information, tout en tenant compte des besoins opérationnels de l'organisation.	Directive fondamentale	Directive facultative	Directive inutile
7.1	Mettre en place un mécanisme officiel d'approbation et d'essai de toutes les connexions externes au réseau.			
7.2	Installer un pare-feu à toutes les connexions Internet.			
7.3	Installer un pare-feu entre la zone démilitarisée et la connexion intranet.			
7.4	Pour les pare-feu, utiliser des configurations multistratifiées pour mieux protéger les renseignements de nature délicate. (Voir l'annexe pour la classification des données délicates.)			
7.5	Valider les configurations des pare-feu au moyen d'outils de mesure de la vulnérabilité disponibles auprès des fournisseurs.			

7.6	Procéder à des évaluations de la sécurité des applications et des bases de données au niveau de la couche application.			

		Directive fondamentale	Directive facultative	Directive inutile
8.0	Installer et configurer des anti-espiogiciels pour assurer une protection maximale des renseignements délicats sur tous les serveurs, ordinateurs personnels et ordinateurs portatifs.			
8.1	Veiller aux téléchargements et mises à jour automatiques de ces logiciels sur les systèmes ou réseaux de l'organisation.			
8.2	Veiller aux téléchargements et mises à jour automatiques de ces logiciels sur les ordinateurs personnels, ordinateurs portatifs et assistants numériques branchés aux systèmes ou réseaux de l'organisation.			
8.3	Effectuer fréquemment le balayage des données entreposées en utilisant des technologies permettant de détecter, de mettre en quarantaine et de supprimer les virus, les vers et les chevaux de Troie.			
8.4	Aviser les employés de ne pas télécharger de pièces jointes de sources inconnues susceptibles de contenir des virus, des vers, des espiogiciels, ou encore des logiciels de reconnaissance de la frappe qui pourraient donner à des personnes non autorisées l'accès aux réseaux de l'organisation. Cela vaut pour les utilisateurs d'ordinateurs ayant accès au réseau de l'organisation, y compris les employés qui travaillent à distance ou ceux qui voyagent et se branchent à partir d'un hôtel ou d'un autre point d'accès public.			

		Directive fondamentale	Directive facultative	Directive inutile
9.0	Installer régulièrement les mises à jour et les correctifs de sécurité des logiciels.			
9.1	Installer les correctifs de sécurité dans le mois suivant leur date de diffusion.			
9.2	Créer un processus pour découvrir les vulnérabilités à mesure qu'elles sont connues en s'abonnant à des services d'alerte qui signalent les menaces externes nouvelles.			
9.3	S'assurer que tous les serveurs disposent bien des dernières versions des applications et des correctifs de sécurité. Faire aussi le balayage des serveurs pour en vérifier la configuration.			

		Directive fondamentale	Directive facultative	Directive inutile
10.0	Renforcer la sécurité des sites Web.			
10.1	Empêcher que les pages Web de l'organisation puissent être transmises en trames à un autre site.			
10.2	Vérifier que toutes les pages Web qui permettent aux utilisateurs de transmettre ou de recevoir des renseignements de nature délicate utilisent https:// ou une autre méthode sécuritaire comme le protocole SSL, ou des sceaux ou des certificats du Web.			
10.3	Masquer les numéros de comptes et de cartes de crédit.			
10.4	Identifier clairement les liens vers des sites tiers pour que les utilisateurs sachent bien qu'ils quittent le site de l'organisation lorsqu'ils suivent les liens en question.			
10.5	Préparer un formulaire de courriel sécurisé pour les utilisateurs éventuels.			

11.0	Lors du développement de logiciels, concevoir et appliquer des méthodes de développement des applications Web axées sur la sécurité.	Directive fondamentale	Directive facultative	Directive inutile
11.1	Dans la mesure du possible, utiliser des outils de travail électroniques de bureau pour valider et corriger les problèmes de codes.			
11.2	Mettre en place un système d'assurance de la qualité et d'essai qui inclut la détection, la mesure et la gestion des problèmes de sécurité.			
11.3	Dans le cycle de développement des logiciels, prévoir une formation sur les outils de sécurité.			
11.4	Concevoir un système d'achat et d'acceptation à mettre en branle pour acheter des logiciels auprès de tiers. Vérifier si le système de codage du fournisseur et du tiers présente un niveau de risque acceptable.			
11.5	Concevoir un système d'activation et d'intégration. S'assurer que les propriétaires du projet évaluent les risques de leurs applications avant de les rendre publiques.			
11.6	Évaluer les applications de chaque code de production existant et chacune des versions produites par le cycle de maintenance.			

Partie 3 : Surveillance matérielle

1.0	Surveiller la légitimité des utilisations et des accès.	Directive fondamentale	Directive facultative	Directive inutile
1.1	Surveiller les activités inhabituelles sur Internet (comme le furetage sur le Web ou l'utilisation de logiciels de partage de fichiers de poste à poste). S'assurer, ce faisant, de tenir compte des restrictions prévues par la loi.			
1.2	Surveiller les courriels inhabituels.			
1.3	Examiner périodiquement ou au hasard les documents et les logiciels contenus dans les ordinateurs portatifs et les assistants numériques distribués par l'organisation.			
1.4	Surveiller l'existence éventuelle de copies piratées ou inactives de logiciels sous licence.			

2.0	Mettre en place des contrôles de l'accès physique.	Directive fondamentale	Directive facultative	Directive inutile
2.1	Installer aux voies d'accès du centre de données des systèmes de reconnaissance du numéro d'identification personnel, des cartes intelligentes ou des lecteurs biométriques.			
2.2	Restreindre l'accès du centre de données aux seules personnes qui ont légitimement besoin d'y travailler.			
2.3	Créer une méthode pour reconnaître les droits d'accès et privilèges des employés.			
2.4	Surveiller de près la distribution des clés et des passe-partout, et surtout des clés maîtresses, et procéder à de fréquentes vérifications.			
2.5	Créer une méthode qui permettra de suspendre des droits d'accès dès qu'on soupçonne fortement un employé ou un agent contractuel de s'être adonné à des activités illicites ou dès qu'il a été reconnu coupable de telles activités.			
2.6	Créer une méthode qui permettra de distinguer les employés des agents contractuels.			

3.0	Installer un poste de contrôle sécuritaire et établir des procédures de surveillance.	Directive fondamentale	Directive facultative	Directive inutile
3.1	Installer un bureau chargé de la réception ou de la sécurité du centre de données, surtout à l'entrée de l'endroit où sont entreposés ou accessibles des renseignements confidentiels ou délicats.			
3.2	Créer une méthode officielle qui guide l'octroi des droits d'accès à ces secteurs et pour tenir à jour la liste des titulaires de ces droits.			
3.3	Surveiller les déplacements de tous les visiteurs en utilisant des badges temporaires ou des supports lisibles par machine (comme des badges d'identification par radiofréquence).			
3.4	Prendre les précautions nécessaires dans les zones où il est possible d'accéder à des données délicates. Cela peut inclure l'installation de verrous spéciaux, la mise en poste de gardiens de sécurité, des contrôles d'accès et autres. Dans les zones névralgiques, comme les centres de données, étudier la possibilité d'installer des détecteurs de mouvement, des microcontacts, des tapis détecteurs et d'autres dispositifs ou mesures pour signaler les ouvertures de portes et les mouvements à l'intérieur.			
3.5	Installer des télévisions en circuit fermé qui permettent de surveiller les points d'entrée.			

4.0	Protéger les installations de données, y compris tous les appareils d'entreposage et l'équipement informatique.	Directive fondamentale	Directive facultative	Directive inutile
4.1	Installer les quais de chargement ou les zones de livraison à un endroit du bâtiment éloigné des zones où l'on traite ou entrepose les renseignements confidentiels.			
4.2	Surveiller ou limiter l'accès aux boîtes de connexion et aux lignes de télécommunications qui passent par le centre de données.			
4.3	Ranger l'équipement particulièrement névralgique dans des pièces qui n'ont ni fenêtres, ni portes, ni puits de lumière, ni mur donnant sur l'extérieur.			
4.4	La zone réservée aux systèmes ou aux réseaux de l'organisation doit être conçue et construite de manière à satisfaire les besoins de sécurité de l'information.			
4.5	Utiliser des zones d'accès restreint et des bacs pour protéger l'équipement délicat. Il importe d'en verrouiller l'accès régulièrement et de conserver les clés en lieu sûr.			
4.6	Utiliser des classeurs verrouillés pour y conserver les imprimés contenant des renseignements délicats ou confidentiels.			
4.7	Obtenir l'approbation écrite du directeur du centre de données avant de débrancher ou de retirer des appareils d'entreposage du système ou du réseau central de configuration des TI.			
4.8	Tenir à jour les méthodes d'enregistrement de tous les appareils et supports d'entreposage amovibles, y compris les bandes magnétiques.			
4.9	Garder les ordinateurs portatifs et autres appareils mobiles inutilisés sous clé pour en prévenir le vol.			
4.10	Prévoir des technologies et d'autres dispositifs pour couper l'accès à distance au cas où un appareil mobile présenterait une menace.			

5.0	Installer et entretenir des systèmes de protection environnementale raisonnables qui protègent tous les actifs du centre de données.	Directive fondamentale	Directive facultative	Directive inutile
5.1	Installer un plancher surélevé pour protéger l'équipement du centre de données.			
5.2	Installer et entretenir des systèmes de détection et d'extinction des incendies.			
5.3	Prévoir un système d'alimentation sans coupure.			
5.4	Utiliser des limiteurs de surtension pour tous les appareils.			

Partie 4 : Plan d'intervention en cas d'incident

1.0	Mettre sur pied une équipe d'intervention interne en cas d'incident.	Directive fondamentale	Directive facultative	Directive inutile
1.1	Créer une équipe d'intervention interne qui aura les compétences, les pouvoirs et les ressources nécessaires pour agir rapidement en cas d'incident menaçant la sécurité. Cette équipe pourrait être chargée d'enquêter sur les causes et les circonstances de l'incident; de limiter les dommages; de recouvrer les données, de décider s'il y a lieu ou non de communiquer avec les autorités policières, de la manière d'agir avec les victimes (comme les clients ou les employés) et de la façon de traiter avec les médias; et de faire un compte rendu une fois l'incident clos. Si cette équipe n'est pas celle qui a préparé les politiques d'intervention en cas d'incident, il importe que les deux groupes entretiennent une relation de travail claire et partagent certains dossiers.			
1.2	Étudier la possibilité d'inclure dans l'équipe des représentants des services suivants : TI, sécurité, protection de la vie privée, services juridiques, service du marketing, des ventes et des relations avec la clientèle (lorsque l'organisation possède des données sur ses clients), ressources humaines (lorsque l'organisation possède des données sur ses employés) et service des relations avec les médias. L'équipe pourrait aussi comprendre des experts de l'extérieur engagés à contrat ou autrement.			
1.3	Définir clairement les rôles et les responsabilités des différents membres de l'équipe.			

2.0	Concevoir et rédiger un plan d'intervention en cas de brèche dans la sécurité.	Directive fondamentale	Directive facultative	Directive inutile
2.1	Dresser la liste des politiques ou procédures d'intervention ou d'enquête en vigueur.			
2.2	Adopter un processus interne à suivre en cas de brèche dans la sécurité indiquant l'ordre des mesures à prendre, les personnes à aviser et les pouvoirs décisionnels. Si un tel processus existe déjà, vérifier s'il est exhaustif et à jour.			
2.3	Créer une capacité d'analyse judiciaire qui soutiendra les enquêtes menées à la suite d'un incident et qui garantira la préservation des preuves possibles. Les organisations de petite et de moyenne taille qui n'ont souvent pas les compétences techniques nécessaires sur place peuvent penser à confier cette fonction à un tiers.			
2.4	Envisager de consulter les autorités policières à l'avance pour bien comprendre la procédure à suivre et les ressources qu'elles pourraient apporter advenant une brèche dans la sécurité. Parmi ces autorités figurent les équipes spécialisées de la criminalité technologique de la localité, le FBI, les services secrets, les services postaux et le National Infrastructure Protection Service.			
2.5	Créer un processus d'évaluation qui guidera la décision de communiquer ou non avec les autorités policières en cas de brèche dans la sécurité et la manière de le faire.			

3.0	Établir un processus de signalement des incidents et d'intervention.	Directive fondamentale	Directive facultative	Directive inutile
3.1	Souligner l'importance de signaler à l'interne toutes les activités douteuses et brèches éventuelles dans la sécurité et s'assurer que tous les employés comprennent le processus interne de notification et sachent, plus précisément, quelles personnes ils doivent aviser en cas d'incident. Par « incident », on entend l'accès non autorisé aux données, ou encore l'obtention ou l'utilisation illicite de ces données. Insister sur la nécessité de signaler tous les accès non autorisés, qu'ils soient internes ou externes.			
3.2	Mettre sur pied des systèmes internes de repérage des brèches réelles ou éventuelles dans la sécurité, évaluer quelle information a pu être obtenue ou consultée et par qui. Les systèmes et procédés doivent aussi envoyer un signal d'alarme en cas d'accès par mégarde à l'information par des employés non autorisés.			
3.3	Prévoir un processus précis de signalement et d'intervention à suivre en cas de vol, de perte ou de disparition d'un ordinateur portatif ou d'un autre appareil mobile. Créer une procédure qui permettra de savoir rapidement quelle information figurait sur l'ordinateur portatif, comment elle était protégée et quels sont les droits d'accès correspondants. Modifier, au besoin, les droits d'accès des utilisateurs finaux.			
3.4	En tant que responsable et partie dans la relation employeur-employé ou avec le client (c'est-à-dire « propriétaire des données »), exiger, par voie de contrat ou autrement, que les fournisseurs de l'organisation (c'est-à-dire les « gardiens des données ») vous avisent immédiatement s'ils prennent connaissance d'une brèche dans la protection de données que vous leur avez fournies ou avez mises à leur disposition. Exiger de ces fournisseurs qu'ils vous tiennent au courant de l'enquête qu'ils mènent et qu'ils travaillent avec vous si vous décidez de faire enquête de votre côté ou pour tout autre suivi de l'incident.			
3.5	À l'inverse, en qualité de fournisseur, prendre connaissance de ses obligations contractuelles ou légales d'aviser le contact en cas de brèche dans la protection des données fournies. Avant de signaler l'incident, s'assurer d'en connaître les détails, qu'on ait ou non l'obligation technique de procéder à ce signalement.			

4.0	Prévoir un examen et des essais périodiques de même qu'un examen et un essai après chaque incident.	Directive fondamentale	Directive facultative	Directive inutile
4.1	Adopter un processus interne de compte rendu après un incident dans le cadre duquel on passera en revue les choses qui n'ont pas marché, on tirera des conclusions pour l'avenir et on établira la marche à suivre dans l'avenir.			
4.2	Documenter en bonne et due forme tous les plans, politiques, processus et systèmes connexes d'intervention et s'assurer que les employés chargés de les mettre à exécution les comprennent. Faire connaître ces plans, politiques, processus et systèmes par des formations et des mises à jour le cas échéant.			
4.3	Revoir, éprouver et mettre à jour, périodiquement et après chaque incident, tous les plans, politiques, processus et systèmes d'intervention.			

Partie 5 : Processus de notification des brèches dans la protection des données

1.0	Mettre en place un processus permettant de déterminer s'il faut ou non envoyer un avis de brèche dans la protection des données, aux termes de la loi ou pour d'autres considérations.	Directive fondamentale	Directive facultative	Directive inutile
1.1	Examiner la possibilité de créer un sous-groupe dans l'équipe d'intervention en cas d'incident ou de nommer un responsable dont le rôle sera d'évaluer, pour chaque incident, la nécessité d'émettre ou non un avis de brèche dans la protection des données et, le cas échéant, d'entamer le processus d'envoi de l'avis. Si on opte pour un seul responsable, prévoir un remplaçant pendant ses congés annuels, ses congés de maladie ou autres absences.			
1.2	Prendre connaissance des lois de l'État sur les notifications de brèches dans la protection des données et autres questions liées à la protection de la vie privée, et des lois internationales pertinentes. Ces lois dictent la conduite à avoir, selon les circonstances, pour la notification des personnes dont les renseignements personnels ont été consultés ou obtenus de manière illicite. Les facteurs à considérer sont la nature de la brèche, le type de renseignements en cause et l'État dont l'organisation relève. (Il importe de noter qu'une loi fédérale est aussi en voie d'être adoptée par le gouvernement américain.)			
1.3	Mettre en place un processus qui permettra de déterminer s'il faut ou non envoyer un avis de brèche dans la protection des données, aux termes de la loi ou pour d'autres considérations.			
1.4	En l'absence d'obligation légale, examiner quand même la possibilité d'envoyer un avis de brèche dans la protection des données, surtout en cas d'accès non autorisé à des données ou d'obtention illicite de données qui pourraient entraîner un préjudice grave pour la personne à qui ces renseignements appartiennent.			
1.5	Dans l'évaluation de ce préjudice grave, se référer aux catégories de données décrites à la fin des présentes lignes directrices.			
1.6	Examiner la possibilité de déterminer à l'avance quelles catégories de données moins délicates ne sont pas susceptibles d'entraîner la notification obligatoire de brèche dans la protection des données. Sous réserve des dispositions de la loi, parmi ces données peuvent figurer des adresses de courriel qui ne sont pas liées à d'autres renseignements personnels.			

2.0	Mettre en place un processus qui permettra de déterminer, une fois établie l'obligation d'émettre un avis, à qui l'avis doit être envoyé.	Directive fondamentale	Directive facultative	Directive inutile
2.1	Déterminer qui sont les personnes touchées et aviser si possible chacune d'elles. Vérifier deux fois la liste des destinataires avant d'envoyer l'avis.			
2.2	Faire en sorte que seules les personnes dont les renseignements personnels sont compromis figurent sur la liste des destinataires. S'il est impossible de déterminer avec précision qui sont les personnes touchées, examiner la possibilité d'aviser tous les membres du groupe concerné, à condition que le risque de préjudice soit supérieur à l'incertitude entourant les personnes réellement touchées.			

3.0	Mettre en place un processus de communication de l'avis de brèche dans la protection des données.	Directive fondamentale	Directive facultative	Directive inutile
3.1	Examiner les différents moyens de communication à utiliser selon les circonstances, par exemple, le moyen utilisé sera différent dans le contexte d'une brèche dans la protection des			

	renseignements personnels des employés par rapport à ceux des clients.			
3.2	Examiner les différents choix possibles si on ne détient pas toute l'information nécessaire pour communiquer directement avec les personnes concernées.			

Partie 5 : Processus de notification des brèches dans la protection des données (suite)

		Directive fondamentale	Directive facultative	Directive inutile
4.0	Tenir compte des facteurs qui influent sur le moment choisi pour émettre un avis de brèche dans la protection des données, notamment :			
4.1	En général, il convient d'aviser le plus rapidement possible les personnes concernées par la découverte d'une infraction, à moins que les autorités policières ne craignent que cet avis nuise à leur enquête. Le Commissariat à la protection de la vie privée de la Californie recommande que l'avis soit donné dans les dix jours suivant la confirmation de la brèche dans la protection des données.			
4.2	Lorsque l'infraction est signalée aux autorités policières, leur demander d'indiquer quand un avis peut être envoyé aux personnes concernées. Envoyer alors l'avis dès que possible, conformément aux lois applicables. Examiner la possibilité de nommer un membre de l'équipe d'intervention pour qu'il ou elle fasse le lien avec les autorités policières. Dans la mesure du possible, obtenir des autorités policières qu'elles confirment leur feu vert par écrit.			
4.3	Envoyer la notification de la manière qui convient aux destinataires. Dans les cas de notification des consommateurs, examiner la possibilité d'envoyer l'avis par la poste ou par courriel.			
4.4	Examiner la possibilité d'émettre un avis public général, sur le site Web de l'organisation ou par la voie des grands médias, si le groupe visé est très large ou pour d'autres raisons.			

		Directive fondamentale	Directive facultative	Directive inutile
5.0	Sensibiliser le personnel et d'autres intervenants, le cas échéant, et coordonner les activités connexes.			
5.1	Sensibiliser le personnel du centre d'appel ou d'autres services à la clientèle au sujet des brèches dans la protection des données pour qu'il puisse aider le cas échéant. Examiner la possibilité de créer un service d'aide ouvert en soirée et la fin de semaine.			
5.2	Si la brèche met en cause des renseignements financiers, examiner la possibilité de notifier les agences d'évaluation du crédit avant d'émettre un avis plus général, pour qu'elles aient le temps de se préparer à répondre aux questions que l'avis pourrait susciter. (On trouvera de l'information sur les grandes agences d'évaluation du crédit à l'adresse http://www.ftc.gov/bcp/conline/edcams/gettingcredit/faqs.html.) Toutefois, ne pas retarder la communication de l'avis sous prétexte de collaborer avec les agences d'évaluation du crédit.			

		Directive fondamentale	Directive facultative	Directive inutile
6.0	Établir le contenu de l'avis de brèche dans la protection des données.			
6.1	Réfléchir au contenu de l'avis de brèche dans la protection des données et s'efforcer d'y mettre l'information la plus utile possible.			

6.2	Dans le cas d'une brèche dans la protection des données de consommateurs, inclure dans la notification : a) la date de l'infraction, b) l'information consultée ou obtenue illicitement et les détails de l'infraction, c) les mesures prises pour remédier au problème, d) le numéro de téléphone sans frais où les gens peuvent appeler pour en savoir davantage et s'ils sont personnellement en cause, e) les moyens qu'ont les consommateurs de se protéger contre le risque de vol d'identité, et f) les coordonnées des grandes agences d'évaluation du crédit.			
6.3	Songer à fournir d'autres renseignements qui pourraient aider les gens dont l'identité a peut-être été volée. Par exemple, il peut être utile de produire une brochure sur la manière d'organiser la surveillance du crédit personnel et de lire le rapport d'une agence d'évaluation du crédit.			
6.4	Songer à offrir aux personnes touchées des services gratuits de surveillance du crédit pendant un an, surtout si l'infraction a mis en cause des numéros d'assurance sociale ou de permis de conduire. (Avant de faire cette offre, il faut savoir que, bien souvent, seuls 25 p. 100 des consommateurs environ l'accepteront.)			
6.5	Songer à inclure sur le site Web de l'organisation des liens vers des organismes utiles : comme les trois grandes agences d'évaluation du crédit (par la voie de la Foire aux questions (FAQ) de la Federal Trade Commission (FTC) à l'adresse http://www.ftc.gov/bcp/conline/edcams/gettingcredit/faqs.html, les organismes gouvernementaux comme la FTC qui traite sur son site du vol d'identité (http://www.ftc.gov/bcp/conline/pubs/alerts/info_compalrt.htm), ou d'autres organismes consacrés au vol d'identité comme l'Identity Theft Resource Center (http://www.idtheftcenter.org/) ou à la protection de la vie privée comme la Privacy Rights Clearinghouse (http://www.privacyrights.org/).			
6.6	Trouver des exemples d'avis de brèche dans la protection des données sur le site Web du Commissariat à la protection de la vie privée de la Californie à l'adresse http://www.privacy.ca.gov/recommendations/secbreach.pdf.			

Appendix

Part 1: Administrative Controls

		Should be required	Should be optional	Not relevant
1.0	**Establish a security committee.**			
1.1	Ensure that the committee is composed of cross-functional members representing different parts of the organization.			
1.2	Create a charter for the security committee.			
1.3	Designate an executive sponsor for security function. The sponsor should also serve as a member of the cross-functional committee.			

		Should be required	Should be optional	Not relevant
2.0	**Establish a formal, written security policy and detailed standard operating procedures.**			
2.1	Ensure that the policy applies to the entire organization or that appropriate policies exist to cover the various operations in the organization, and that they are integrated with other enterprise policies. Ensure that appropriate policies also apply to your internal and external websites.			
2.2	Align the policies with other compliance policies, especially those for privacy and secure vendor relationships. Before creating your policies, determine regulatory compliance needs as relevant to the data and customers.			
2.3	Ensure that versions of the security policy are coordinated and rigorous version control is exercised.			
2.4	Periodically review the security policy and standard operating procedures, revising them as necessary based on changing business, technology and environmental conditions.			
2.5	Disseminate the security policy and detailed standard operating procedures to all relevant stakeholders within the organization. Consider developing an externalizable version of the policy and for outside stakeholders of the organization, including outside contractors agents.			
2.6	Provide appropriate information on how you secure information to users on your websites through a link on each page. Consider including this summary in your privacy statement.			

Part 1: Administrative Controls, cont.

		Should be required	Should be optional	Not relevant
3.0	**Conduct ongoing security risk assessments.**			
3.1	Identify and prioritize security risk threats and vulnerabilities. Consider, at a minimum, risks in these areas: employee training and management; information systems; and prevention, detection and response to attacks or other systems failures.			
3.2	Prioritize resource allocation and spending based on prioritized risk areas.			
3.3	Periodically review risk assessments and revise them as necessary, especially in response to business, technology and environmental changes.			

		Should be required	Should be optional	Not relevant
4.0	**Require a system security plan for every major system and network.**			
4.1	Conduct a periodic review of system security plans and revise them as necessary.			
4.2	Ensure that plans and policies for security include periodic review and control over endpoints such as desktop PC's, laptops, PDA's, and other devices which connect to sensitive networks or systems (including Bluetooth technology).			
4.3	Require system interconnection agreements.			
4.4	Require user system access agreements.			
4.5	Conduct periodic review of system interconnection agreements and revise them as necessary.			

		Should be required	Should be optional	Not relevant
5.0	**Establish contingency plans, including maintenance of access controls.**			
5.1	Establish business continuity plan.			
5.2	Establish disaster recovery plan.			
5.3	Establish personnel emergency plan.			
5.4	Conduct periodic review and test of contingency plans and revise them as necessary.			

		Should be required	Should be optional	Not relevant
6.0	**Integrate security throughout the system life cycle, including:**			
6.1	Requirements definitions.			
6.2	Design/procurement procedures.			
6.3	Testing and maintenance procedures.			

Part 1: Administrative Controls, cont.

		Should be required	Should be optional	Not relevant
7.0	**Establish formal data backup processes.**			
7.1	Ensure that data backup includes the maintenance of current access controls.			
7.2	Conduct periodic review and test of data backup processes and revise them as necessary.			

		Should be required	Should be optional	Not relevant
8.0	**Establish security auditing process.**			
8.1	Conduct periodic reviews of all security controls through internal or external audit. Include web applications, as well as host, network and user accounts as part of the audit.			
8.2	Conduct mock reviews to test the organization's ability to respond to threats (including vulnerability to social engineering).			

		Should be required	Should be optional	Not relevant
9.0	**Document all system and network configurations.**			
9.1	Establish a formal configuration/change control process (including vulnerability identification and patching), with pre-production testing.			
9.2	Document and classify all sensitive information (data inventory).			
9.3	Document formal and appropriate rules of behavior, acceptable use and confidentiality agreements for all personnel with access to sensitive information.			
9.4	Document all appropriate separation of duties (e.g., system administrators and security administrators should not be the same person).			
9.5	Document routine and emergency access termination procedures.			
9.6	Document a formal incident response capability.			

		Should be required	Should be optional	Not relevant
10.0	**Establish employee awareness and training program.**			
10.1	Establish a certification and accreditation (C&A) process for employees with access to major systems.			
10.2	Require all employees to undergo basic initial and refresher security training. Track and document completion of training.			
10.3	Support continuing professional training and education for security specialists.			

Part 1: Administrative Controls, cont.

		Should be required	Should be optional	Not relevant
11.0	**Establish special procedures for outsourced IT or data management activities.**			
11.1	Perform vendor due diligence before sharing sensitive or confidential information, including all personally identifiable consumer or employee data.			
11.2	Perform a site audit of the vendor's data center to determine adequacy of security infrastructure.			
11.3	Obtain certification from the vendor that they are in compliance with the customer's privacy and data protection obligations as required by law or stated policies.			
11.4	Impose contractual control over vendors' data use and practices.			
11.5	Perform periodic or random audits of the outsourcing vendor.			
11.6	Whenever feasible, determine the adequacy and competence of the outsourced vendor's key personnel (especially those individuals who are responsible for handling or managing sensitive personal information).			

Part 2: Technical Security

	Control access to information that resides on data storage devices such as servers, desktop PCs, laptops, and PDAs.	SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
1.0				
1.1	Use unique ID or username for all system users. Ensure that neither Social Security nor account numbers are used as an ID or username.			
1.2	Use authentication mechanisms, such as passwords, tokens, and/or biometrics.			
1.3	Require system administrators to use regular user accounts for work that does not need enterprise-wide system or security administration privileges.			
1.4	Assign access privileges based on a need to know (the level of access should only relate to job function and be not based on organizational position or rank).			
1.5	Whenever feasible, utilize a two-factor authentication procedure before granting access to a user's sensitive information.			
1.6	When possible, implement a method for online service requests concerning changes in usernames and passwords.			
1.7	Force appropriate session timeouts, such as 15 minutes or less, if idle.			

	Establish password usage policy that encompasses the following rules:	SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
2.0				
2.1	Whenever feasible, use a minimum of six digit alpha-numeric format. Instruct users to create such passwords during a periodic password change process.			
2.2	Prohibit passwords based on account number, username, real name, Social Security number, or publicly available personal details (birthdays, names of children or pets, etc.).			
2.3	Restrict password reuse.			
2.4	Establish a formal user authentication process for resetting passwords. When possible, make password change or reset option available from the login page. Allow users to update their password hints or questions.			
2.5	When sending a registration confirmation or other type of welcome email, provide only the username within the email and implement a password reset feature on the web site.			
2.6	Username and passwords should not be sent together within the same email.			
2.7	Force password expiration.			
2.8	Establish lost/stolen laptop procedures, including password cancellation.			

Part 2: Technical Security, cont.

		Should be required	Should be optional	Not relevant
3.0	**Control access to information that can be displayed, printed, and/or downloaded to external storage devices, especially desktop PCs, laptops or PDAs.**			
3.1	Have operating controls that restrict downloads of sensitive information without proper identification. (See Appendix for sensitive data classifications.)			
3.2	Have screen savers and screen shields to minimize the display of sensitive data to unauthorized users.			
3.3	Have shutdown controls when computers are idle or inactive.			
3.4	Whenever feasible, only allow read-only access rights when using remote computers or wireless devices to enter the organization's network or enterprise system.			
3.5	As much as possible, limit the use of personally identifiable information on laptops. Where such use is essential, ensure that data is encrypted or, at a minimum, that such laptops are protected by something stronger than a password.			
3.6	Set up periodic disk clean-up reminders to help eliminate temporary backups and empty recycle/trash bin. Consider reflecting this practice in your company document retention/deletion plans.			

		Should be required	Should be optional	Not relevant
4.0	**Monitor user accounts to identify and eliminate inactive users, specifically:**			
4.1	Accounts that have been inactive for 60 days should be automatically terminated.			
4.2	Accounts of terminated employees and contractors should be shut down within 24 hours.			
4.3	Regularly cross-check user accounts against HR records to ensure that access by former employees has been terminated.			

		Should be required	Should be optional	Not relevant
5.0	**Ensure sufficient safeguards over the transmission and storage of data, including:**			
5.1	Use reasonable encryption methods when transmitting or receiving sensitive information, especially when sent or received over the public Internet. Ensure that you employ at least 128-bit encryption.			
5.2	Use wireless encryption protocol (WEP) when transmitting or receiving sensitive information from PDAs, Web phones, laptops, and emerging devices that use Bluetooth connection technologies.			
5.3	Use reasonable encryption methods for storage, especially when maintaining sensitive information on servers, desktop PCs, and laptops.			
5.4	Use VPN software to authorize and encrypt traffic from authorized devices, and ensure that VPN access has adequate controls and is monitored.			
5.5	Use configuration monitoring tools to flag storage devices that are removed from the network or enterprise system.			
5.6	Restrict the downloading of sensitive personal information from central storage devices onto personal computers or wireless storage devices.			

Part 2: Technical Security, cont.

	Configure all servers, desktop PCs, and laptops prior to use, including:	Should be required	Should be optional	Not relevant
6.1	Disable unused ports.			
6.2	Install/enable automatic screen locks to prevent access after a certain period of inactivity.			
6.3	Change all vendor-supplied default passwords.			
6.4	Ensure that wireless encryption protocol (WEP) is enabled prior to allowing wireless devices to be connected to enterprise systems or networks.			
6.5	Treat all internal wireless connections as external connections.			
6.6	Routinely check for unauthorized external access capability, including wireless access points.			
6.7	Confirm that default software installations and configurations are appropriate for your security needs, including as appropriate changing default passwords and appropriately adjusting security parameters.			

	Firewalls should be configured to provide maximum protection over information, balancing business needs with reasonable security.	Should be required	Should be optional	Not relevant
7.1	Establish a formal process for approving and testing all external network connections.			
7.2	Establish a firewall at each Internet connection.			
7.3	Establish a firewall between any DMZ and Intranet connection.			
7.4	Utilize multi-layered firewall configurations to protect sensitive information. (See Appendix for senitive data classification).			
7.5	Validate firewall configurations with vulnerability tools available from vendors.			
7.6	Conduct application level assessments to ensure application and database security.			

	Install and configure anti-spyware software to provide maximum protection of sensitive information on all servers, desktop PCs, and laptops.	Should be required	Should be optional	Not relevant
8.1	Ensure automatic downloads and updates to enterprise system or network.			
8.2	Ensure automatic downloads and updates to desktop PCs, laptops and PDAs that are connected to the enterprise system or network.			
8.3	Perform frequent scans of data storage using enabling technologies to detect, quarantine, and remove viruses, worms, and Trojans.			
8.4	Instruct employees not to download unknown attachments that could contain viruses, worms, spyware or keystroke loggers potentially giving unauthorized individuals access to the company's network. This applies to the user of any computer that has access to the organizational network, including the home computer of a telecommuting employee or a traveling employee logging in from a hotel or other public access point.			

Part 2: Technical Security, cont.

	9.0 Implement security software updates and patches in a timely manner.	SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
9.1	Install security patches within one month of release date.			
9.2	Establish a process to identify newly discovered security vulnerabilities by subscribing to alert services that report current external threats.			
9.3	Ensure that all servers are up-to-date with respect to application version and security patches. Additionally, scan servers for configuration issues.			

	10.0 Enhance the security of your websites.	SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
10.1	Prevent your web pages from being delivered into frames by another site.			
10.2	Ensure that all web pages that enable users to transmit or receive sensitive information use https:// or another security method such as SSL, Web seal, or certificates.			
10.3	Mask account and credit card numbers.			
10.4	Clearly label links to third-party sites to ensure users know they are leaving your site by following the link.			
10.5	Make a secure email form available to prospective users.			

	11.0 When developing software, create and implement security-focused web application development procedures.	SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
11.1	When possible, use desktop tools to validate and correct code issues.			
11.2	Implement quality assurance and testing procedures. This would include detecting, measuring, and managing security defects as part of QA.			
11.3	Include training on security tools as part of the software development life cycle.			
11.4	Develop procurement and acceptance procedures to apply when purchasing third party software. Validate vendor and third party code for acceptable risks.			
11.5	Develop staging and integration procedures. Make sure project owners evaluate application risks before public release.			
11.6	Conduct ongoing application assessments for existing production code and one for each maintenance cycle release.			

Part 3: Physical Controls

	1.0 Monitor legitimate use and access.	Should be required	Should be optional	Not relevant
1.1	Conduct surveillance of unusual Internet activities (such as Web browsing or use of peer-to-peer file sharing software). Be sure to consider any applicable legal restrictions on doing so, however.			
1.2	Conduct surveillance of unusual email.			
1.3	Perform periodic or random reviews of documents and software contained on company issued laptops computers and PDAs.			
1.4	Monitor software licenses for inactive or pirated copies.			

	2.0 Establish physical access controls.	Should be required	Should be optional	Not relevant
2.1	Install PIN devices, smart cards, and/or biometric readers at physical entrances to the data center.			
2.2	Restrict physical access to the data center to only those people who have a legitimate business need.			
2.3	Establish a method to recognize employee access rights and privileges.			
2.4	Keys and passes, especially master keys, should be carefully controlled with frequent reviews and reconciliation.			
2.5	Establish a method to terminate access rights once employee or contractor illegal activities are detected or strongly suspected.			
2.6	Establish a method to differentiate employees from contractors.			

	3.0 Install secure checkpoint review and monitoring procedures.	Should be required	Should be optional	Not relevant
3.1	Implement a data center security or reception desk, especially at the entrance where sensitive or confidential information is housed or is accessible.			
3.2	Implement a formal process for granting access to those areas and for maintaining the list of people with physical access.			
3.3	Identify and monitor the movement of all visitors by using temporary badges or machine readable devices (such as RFID tags).			
3.4	Take appropriate security precautions in areas where access to sensitive data may be had. These can include special locks, security personnel, access controls, and other features. In the most sensitive areas, such as data centers, consider installing motion detectors, micro-switches and pressure pads or other equipment or measures in data centers to indicate when doors are opened or rooms entered.			
3.5	Install closed circuit television to monitor all entry points.			

Part 3: Physical Controls, cont.

	Secure the data facility, including all storage devices and computer equipment.	SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
4.0				
4.1	Locate loading docks or delivery areas in a remote area of the building far away from areas processing or storing confidential information.			
4.2	Control or limit access to junction boxes and telecommunication lines that enter or exit the data center.			
4.3	Rooms that house especially sensitive equipment should have no external walls, doors, windows or sky lights.			
4.4	The area designated for the enterprise system or networks should be designed and built to support the organization's requirement for information security.			
4.5	Secure cages and racks should be used to protect sensitive equipment. These should be locked routinely and keys carefully controlled.			
4.6	Use locked cabinets to store printouts containing sensitive or confidential information.			
4.7	Require documented approval by the data center's management before disconnecting or removing storage devices from the central IT configuration or system network.			
4.8	Maintain logging procedures for all removable storage devices and media, including magnetic tapes.			
4.9	Keep unused laptops and other mobile devices in a locked location to prevent theft.			
4.10	Consider technologies and implementations that can effectively terminate remote access in case of compromised mobile equipment.			

	Install and maintain reasonable environmental protections over all data center assets.	SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
5.0				
5.1	Install raised floor to protect equipment in the data center.			
5.2	Install and maintain fire detection and suppression systems.			
5.3	Implement uninterruptible power supply (UPS).			
5.4	Use surge protectors on all equipment.			

Part 4: Incident Response Plan

	1.0 Establish an internal incident response team.	SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
1.1	Create an internal response team with the expertise, authority, and resources to act quickly in case of a security incident. Possible responsibilities will include investigation of the cause and parameters of the incident; containing and controlling of the incident; data recovery; decisions about external communications to law enforcement, impacted individuals such as customers or employees, and/or the media; and subsequent debriefing after any incident. Assuming this is a different group than is drafting your incident response policies, the two groups must have a clear working relationship and at least some overlap.			
1.2	Consider including representatives from these departments: IT, security, privacy, legal, marketing/sales/customer relations (in case customer data is involved), human resources (in case employee data is involved), and media relations. The team may also include outside experts under retainer or contract.			
1.3	Establish clear roles and responsibilities for all team members.			

	2.0 Establish a formal, written breach response plan.	SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
2.1	Inventory any existing response or investigative policies or related procedures.			
2.2	Implement an internal escalation, notification, and decision making process to be followed in case of a potential security breach. If an established process already exists, review for completeness and currency.			
2.3	Implement a forensic analysis capability to support incident investigations, ensuring that potential evidence is not compromised. Small or medium companies with less internal technical expertise may wish to retain a third party expert for this function.			
2.4	Consider consulting with law enforcement resources in advance of any incident to understand relevant procedures and what resources they may bring to bear, should a breach occur. Appropriate law enforcement resources may include your local high tech crimes task force, FBI, Secret Service, US Postal Service, and the National Infrastructure Protection Service.			
2.5	Establish a process for assessing whether to contact law enforcement in case of a breach, and for making such contact.			

Part 4: Incident Response Plan, cont.

	Develop a process for reporting and escalating incidents.	Should be required	Should be optional	Not relevant
3.1	Emphasize that all suspicious activity and potential breaches should be reported internally, and ensure that all employees understand the internal notification process, specifically, who within the company they are to report a potential incident to. "Incidents" include unauthorized access, acquisition or use. Emphasize that both internal and external unauthorized access should be reported.			
3.2	Develop internal systems and processes to identify breaches and potential breaches, assessing what information may have been accessed or acquired and by whom. Systems and processes may also raise alerts when inadvertent access to information is made by unauthorized employees.			
3.3	Implement a specific notification and escalation process for when a laptop or other mobile device is lost, missing or stolen. Establish a procedure to understand what information was on the laptop, how it was secured and what access rights may exist; modify end-user access rights as needed.			
3.4	In your role as a principal and the party with the customer or employer-employee relationship (the "data owner"), you should require, e.g., via contract, that any outside vendors ("data custodians") notify you immediately upon detection of a breach involving data that you have provided to them or otherwise made accessible to them. Require such vendors to keep you informed of the investigation process and progress and to work cooperatively with you in any investigation or other follow-up activity.			
3.5	Conversely, if you are a vendor, be aware of any contractual or legal obligation you may have to notify your principal of a breach involving data they have provided to you. Consider providing such notice once you have established the facts of the breach, regardless of whether you have a technical obligation to do so.			

	Establish a periodic and post-incident review and re-testing process.	Should be required	Should be optional	Not relevant
4.1	Establish a post-incident internal debriefing process, including what went wrong, lessons learned and next steps.			
4.2	All incident plans, policies, processes, and related systems should be appropriately documented and understood by the responsible employees. Communicate these through training and updates as appropriate.			
4.3	All incident plans, policies, processes, and related systems should be reviewed, tested and updated, both periodically and after any incident.			

Part 5: Breach Notice Processes

		Should be required	Should be optional	Not relevant
1.0	**Establish a process for assessing whether a breach notice is either legally mandated or otherwise appropriate.**			
1.1	Consider establishing a breach notice subgroup of your incident response team—or designate an individual—tasked with assessing, in case of a breach, whether the need for a breach notice has been triggered and, if so, carrying out the breach notice process. If assigned to an individual, designate a substitute in case of vacation, illness or absence for any reason.			
1.2	Familiarize yourself with applicable state breach notice and other privacy-related laws, as well as any relevant international laws. Such laws mandate, under certain circumstances, that you notify individuals whose personally identifiable information has been accessed or acquired in an unauthorized fashion. Factors impacting such legal requirements will include the nature of a breach, the type of information involved, and the jurisdictions impacted. (Note that federal legislation is also pending.)			
1.3	Establish a process for determining whether notice is legally mandated or otherwise appropriate.			
1.4	If notice is not legally mandated, consider nonetheless providing notice, particularly where there has been unauthorized access or acquisition of data that could reasonably result in material harm to the subject of the information.			
1.5	When evaluating such a possibility of material harm, consider using the "sensitive data" category as defined in the "Data Categories" chart at the bottom of these Guidelines.			
1.6	Consider establishing, also, what less-sensitive categories of data will likely not trigger a breach notice. Depending on applicable legal requirements, examples might include email addresses not linked to any other personally identifiable information.			

		Should be required	Should be optional	Not relevant
2.0	**Establish a process for determining who to notify, once the need for a breach notice has been triggered.**			
2.1	Determine who has been affected, and notify each affected individual when possible. Doublecheck the list of recipients before sending.			
2.2	Try to ensure that only those individuals whose personally identifiable information was compromised are included in the group to be notified. If you cannot determine the exact individuals affected, consider notifying all members of the group affected if the likelihood of material harm outweighs the uncertainty that the individuals were affected.			

		Should be required	Should be optional	Not relevant
3.0	**Establish a process for communicating a breach notice.**			
3.1	Consider potential communication channels for different circumstances, e.g., your plan may be different for an employee vs. a customer data breach.			
3.2	Consider available options, should you not have complete contact information for all impacted individuals.			

Part 5: Breach Notice Processes, cont.

	4.0 Considerations that affect the timing of a breach notice include:	SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
4.1	In general, notify affected individuals as soon as reasonably possible after a breach is discovered, unless law enforcement officials indicate that notice would impede their investigation. Note that the California Office of Privacy Protection recommends notification within ten days once a breach has been confirmed.			
4.2	If you have reported the breach to law enforcement, ask them to inform you when it is safe to notify affected individuals. Send out notice as soon as practicable and in compliance with existing notification laws when so informed. Consider appointing a member of the response team to follow up with law enforcement in order to find out when it is safe to notify the affected individuals. When possible, get such confirmation in writing.			
4.3	Send the notification in an appropriate manner to the intended audience. In consumer notification cases, consider notice by traditional mail and by email where appropriate.			
4.4	Consider the option of giving general public notice, on your website and/or through major media, where the group to be notified is very large or it is otherwise appropriate.			

	5.0 Educate and coordinate with your own and other potential resources.	SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
5.1	Educate your call center staff or other customer service employees about the breach so they can provide knowledgeable assistance. Consider having assistance available evenings and weekends.			
5.2	If the breach involves financial information, consider notifying credit reporting agencies before sending out notice of a breach to a large number of individuals, so they can prepare for the consequent inquiries. (You will find information about the major CRAs at http://www.ftc.gov/bcp/conline/edcams/gettingcredit/faqs.html.) However, do not delay notice to individuals because of cooperation with credit reporting agencies.			

Part 5: Breach Notice Processes, cont.

6.0	Content of breach notice communication.	SHOULD BE REQUIRED	SHOULD BE OPTIONAL	NOT RELEVANT
6.1	Consider carefully the content of any breach notice communications, and focus on providing the most useful information possible.			
6.2	In the case of consumer breach, notification should include: (a) the date of the breach; (b) what information was accessed and pertinent details about the breach; (c) remedial actions taken; (d) your toll-free number for individuals to call to learn more, including whether or not that individual's data may be at risk; (e) how affected individuals may protect themselves against the possibility of identity theft; and (f) contact information for major credit reporting agencies.			
6.3	Consider providing further information that might be helpful for those who believe they maybe a victim of identity theft. For example, including a brochure about how to set up credit monitoring or how to read a credit report could be helpful.			
6.4	Consider offering free credit monitoring services for one year to affected individuals, particularly if the incident involved Social Security or Driver's License numbers. (When considering making such an offer, note that often only about 25% of consumers will accept such an offer.)			
6.5	Consider providing links on your website to resources such as the following: the three major credit reporting agencies (available via an FTC "FAQ" at http://www.ftc.gov/bcp/conline/edcams/gettingcredit/faqs.html); to government agency resources such as this FTC identity theft consumer alert (http://www.ftc.gov/bcp/conline/pubs/alerts/info-compalrt.htm); and/or to identity theft resources such as the Identity Theft Resource Center (www.idtheftcenter.org/) or the Privacy Rights Clearinghouse (http://www.privacyrights.org/).			
6.6	You will also find sample breach notices letters provided by the California Office of Privacy Protection available at: http://www.privacy.ca.gov/recommendations/secbreach.pdf.			

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

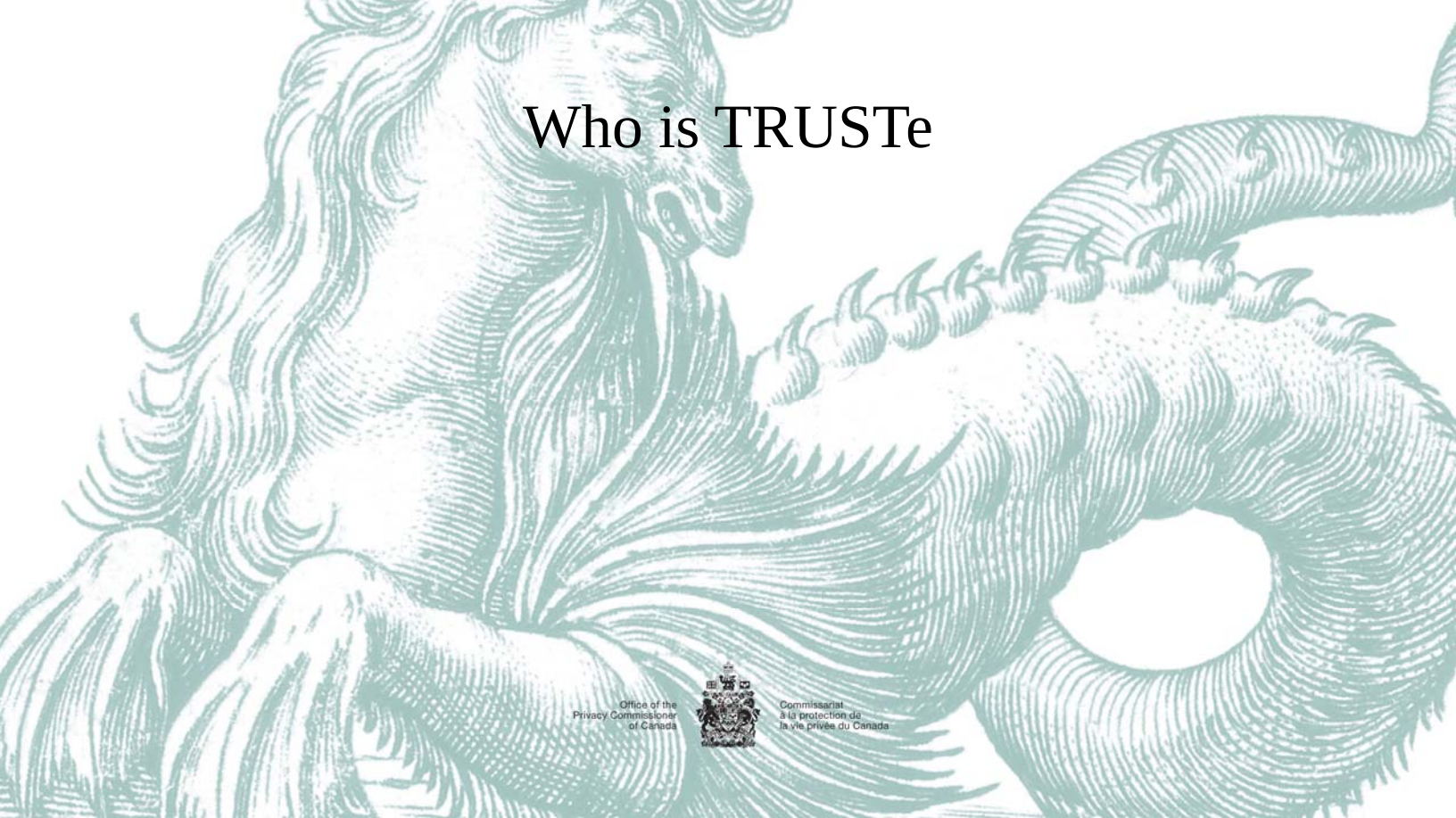
TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Qu’est-ce que TRUSTe ?

Who is TRUSTe



Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

De nombreuses entreprises de premier plan mondial préservent la vie privée de leurs clients grâce à TRUSTe, parmi lesquelles :

AOL, Apple Computer, AT&T, DoubleClick, eBay, E-LOAN, Gateway Computers, IBM, Intel, InterContinental Hotels Group, Intuit, Microsoft, Nestlé, NFL, Monster, New York Times, Digital, Oracle, Pfizer, The Weather Channel, Verizon, Wireless, Walt Disney, Internet Group, WebMD, Yahoo!

Qu'est-ce que TRUSTe?

TRUSTe travaille sur l'amélioration de la protection des données personnelles et de la confiance dans un monde réseauté. Grâce à ses labels de protection des données personnelles sur le Web et de protection des données personnelles dans le courrier électronique de même qu'à son Programme de téléchargement fiable, TRUSTe aide les consommateurs et les entreprises à distinguer les organisations en ligne dignes de confiance. TRUSTe est un organisme indépendant à but non lucratif fondé en 1997; il homologue plus de 2 500 sites Web, y compris des portails Internet et des marques de premier plan comme Microsoft, IBM, Oracle, Nestlé, Intuit et eBay. De plus, TRUSTe règle des milliers de litiges concernant la protection de la vie privée chaque année. Afin d'en savoir plus sur la protection des données personnelles sur Internet, on peut visiter le site www.truste.org.

Quels sont les avantages offerts par TRUSTe?

- Bâtir un climat de confiance en distribuant des labels fiables aux produits.
- Augmenter les conversions, les enregistrements et l'engagement auprès des consommateurs.
- Permettre aux organisations de rester en conformité avec les lois sur la protection des données personnelles tant au niveau national qu'au niveau des États.
- Repérer les failles dans la protection des données personnelles avant qu'elles ne soit effectives, grâce à un balayage et à une surveillance automatique par MAXAMINE.
- Résoudre les litiges avec les consommateurs en adoptant une position de tierce partie pour régler ces litiges.

Many of the world's leading companies and organizations protect the privacy of their customers with TRUSTe, including:

AOL, Apple Computer, AT&T, DoubleClick, eBay, E-LOAN, Gateway Computers, IBM, Intel, InterContinental Hotels Group, Intuit, Microsoft, Nestle, NFL, Monster, New York Times, Digital, Oracle, Pfizer The Weather Channel, Verizon, Wireless, Walt Disney Internet Group, WebMD, Yahoo!

Who is TRUSTe?

TRUSTe works to advance privacy and trust for a networked world. Through its Web Privacy Seal, Email Privacy Seal, and Trusted Download Program, TRUSTe helps consumers and businesses identify trustworthy online organizations. An independent, nonprofit organization founded in 1997, TRUSTe certifies more than 2,500 Web sites, including the major internet portals and leading brands such as Microsoft, IBM, Oracle, Nestle, Intuit and eBay. In addition, TRUSTe resolves thousands of individual privacy disputes every year. To learn more about internet privacy visit www.truste.org

What are the benefits of TRUSTe?

- Build trust and confidence by displaying trusted consumer facing seals.
- Increase conversions, registrations, and engagement with customers.
- Stay compliant with national and state privacy laws.
- Uncover privacy pitfalls before they occur through automated MAXAMINE scanning and monitoring.
- Alleviate disputes with consumers through third party dispute resolution.
- Improve your search ranking and reputation-with TRUSTe seal notation in browsing tools.
- Receive guidance in developing your online-privacy practices.

TRUSTe programs

Web Privacy Seal
Marks companies that adhere to TRUSTe's strict privacy principles and comply with the TRUSTe

- Améliorer la visibilité et la réputation des organisations sur les moteurs de recherche grâce au label TRUSTe
- Proposer des lignes directrices dans l'élaboration de bonnes pratiques de protection des données personnelles en ligne.

Programmes TRUSTe

Label de protection des données personnelles en ligne.
Labellisation des entreprises qui adhèrent aux principes stricts de protection des données personnelles de TRUSTe et sont en conformité avec le Programme de surveillance de TRUSTe pour la résolution des litiges.

Label de protection des données personnelles dans le courrier électronique
Renforcement de l'engagement des entreprises en matière de bonnes pratiques pour le courrier électronique, en accréditant les politiques de divulgation des courriels, de respect de la réputation et de désabonnement.

Programme de téléchargement fiable
Ce programme incite les fabricants de logiciels publicitaires ou autres à faire connaître de façon claire et incontournable les fonctionnalités clés de leur logiciel et à obtenir le consentement éclairé des consommateurs avant le téléchargement.

Caractéristiques de TRUSTe

Processus d'homologation de TRUSTe
Les candidats complètent une auto-évaluation décrivant leur manière de recueillir, d'utiliser et de traiter les informations. Les gestionnaires de clientèle comparent toutes ces évaluations aux procédures réellement suivies et aux divulgations réellement faites sur le site Web grâce à un examen général du site. Les candidats reçoivent un rapport détaillé des constatations, qui donne les résultats de l'examen général et établit la liste des actions à mener pour se mettre en conformité avec les normes du Programme.

Labels TRUSTe
À la suite de leur homologation, les membres reçoivent des labels TRUSTe identifiant les sites sécurisés, à afficher sur leurs pages Web. Les gestionnaires de la clientèle aident les clients à placer au mieux les labels, pour maximiser leur

Watchdog Dispute Resolution System.

Email Privacy Seal
Reinforces companies' commitments to good email practices by certifying email disclosures, reputation, and unsubscribe policies.

Trusted Download Program
Provides market incentives for adware and other software companies to clearly and unavoidably communicate key functionalities and obtain informed consumer consent prior to download.

TRUSTe Features

TRUSTe certification process
Applicants complete a self-assessment detailing information collection, use, and procedures. Client services managers review all self-assessments against actual Web site procedures and disclosures with a site walkthrough. Applicants receive a detailed site findings report which identifies the results of the site walkthrough and lists action items for the applicant to complete to become compliant with program standards.

TRUSTe seals
After passing the certification process, members receive TRUSTe's trusted web seals to display throughout their respective web pages. Client services managers provide seal placement guidance to ensure members are maximizing the impact of the seals. More than one million consumers click on these seals per month to confirm TRUSTe membership.

Monitoring and Scanning
TRUSTe uses a combination of tools including MAXAMINE scanning technology and personal attention to monitor licensed sites for breaches of their privacy policies. Compliance analysts look for things such as encryption measures on sensitive pages and undisclosed "cookies", or single-pixel tracking devices. Oftentimes, violations are unintentionally introduced when organizations update their pages, undergo changes in ownership, or launch new initiatives such as contests or newsletters.

Watchdog Dispute Resolution System
The TRUSTe Watchdog Dispute Resolution System is an online tool that allows consumers to report violations of posted privacy statements, or specific privacy concerns pertaining to TRUSTe

impact. Plus d'un million de consommateurs cliquent chaque mois sur ces labels pour vérifier l'adhésion d'une entreprise à TRUSTe.

Surveillance et balayage
TRUSTe utilise un ensemble d'outils, dont la technologie de balayage MAXAMINE et sa propre vigilance, pour surveiller les sites homologués et détecter les failles dans leur politique de confidentialité. TRUSTe recherche par exemple les mesures de cryptage des pages au contenu délicat et les témoins de connexion cachés ou les dispositifs de repérage à pixel unique. Il arrive souvent que des irrégularités surviennent par accident, lorsque les organisations mettent leur site à jour, changent de propriétaire ou lancent de nouvelles activités comme un concours ou un bulletin d'information.

Procédure de surveillance pour la résolution des litiges
La procédure de surveillance de TRUSTe pour la résolution des litiges est un outil en ligne qui permet aux consommateurs de signaler les infractions aux règles affichées de protection des données personnelles ou les sujets d'inquiétude particuliers sur la protection des données personnelles, visant les sites Web membres de TRUSTe.

Protection du label
Pour préserver la volonté des entreprises sous licence TRUSTe de se conformer à des normes strictes et pour garantir la conformité constante à ces normes, TRUSTe protège vigoureusement ses labels. TRUSTe conserve une « liste noire » des sites Web usurpant le label sur son site Web TRUSTe.org.

Le processus TRUSTe

1 L'organisation complète un contrat TRUSTe et une auto-évaluation.

2 TRUSTe effectue un premier examen du site et donne une série de recommandations écrites sous forme de rapport détaillé des constatations.

3 L'entreprise met en œuvre les recommandations sur son site.

4 TRUSTe décerne à l'entreprise des labels de protection de la vie privée. Ceux-ci doivent

member Web sites.

Trademark Enforcement
To protect the investment of TRUSTe licensees to meet strict standards, and to ensure ongoing compliance, TRUSTe vigorously enforces trademarks. TRUSTe maintains a "blacklist" of trademark violator Web sites on the TRUSTe.org Web site.

The TRUSTe Process

1 your organization fills out a TRUSTe contract and self-assessment.

2 TRUSTe conducts an initial site walkthrough and provides a set of written recommendations in the form of a site findings report.

3 you implement recommendations on your website.

4 TRUSTe awards you privacy seals. Display these where you collect information to build confidence with customers.

5 TRUSTe ensures ongoing compliance and monitoring with MAXAMINE scanning and the TRUSTe watchdog Dispute resolution system.

être affichés sur les pages où l'information est recueillie pour que le consommateur se sente en confiance.

5. TRUSte garantit une conformité et une surveillance par balayage constantes ainsi que la fourniture de la Procédure de surveillance pour la résolution des litiges.

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Présentation du Programme de téléchargement fiable de TRUSTe (phase Bêta)

Introducing TRUSTe Trusted Download Program (Beta)

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Environnement

De nos jours, si un ordinateur est connecté à Internet, il est possible d'y télécharger et d'y installer des logiciels sans avertissement ni consentement préalables. Il est compréhensible que les consommateurs soient fâchés lorsqu'ils découvrent des logiciels malvenus dans leur ordinateur. Dans certains cas, l'application fournit une plus-value indéniable, mais bien souvent, le logiciel peut être considéré comme un « logiciel espion ». Le manque de normes et de définitions a rendu la distinction difficile, aussi bien pour les consommateurs que pour les entreprises, entre un « logiciel espion » et un logiciel légitime. Par conséquent, à la perspective de télécharger des logiciels faciles d'emploi et de valeur s'oppose un profond manque de confiance.

La surveillance par TRUSTe

TRUSTe, le premier organisme d'homologation de la protection des données personnelles en ligne, s'est associé avec les plus grands portails de consommateurs en ligne et d'autres industriels majeurs afin de développer des normes et un programme d'homologation visant les logiciels téléchargeables.

TRUSTe et ses commanditaires ont établi les objectifs suivants :

- améliorer notablement l'expérience des consommateurs à l'égard des logiciels téléchargeables;
- établir les premières normes couvrant l'industrie toute entière à l'intention des développeurs d'applications téléchargeables;
- cibler et développer des applications fiables pour les distributeurs et les mercaticiens;
- protéger les marques publicitaires en ligne agréées en leur permettant de déterminer quelles applications sont fiables et lesquelles ne le sont pas.

Le Programme d'homologation du téléchargement fiable offre des normes rigoureuses, une vérification complète, une surveillance continue, des mécanismes d'obligation et de puissantes incitations du marché.

Le Programme est aujourd'hui en phase Bêta et il dressera une liste blanche des applications se conformant aux exigences de l'homologation, ce qui fournira aux portails de consommateurs et aux

Background

Today, if a computer is connected to the internet, software may be downloaded and installed on it without notice or consent. Consumers are understandably frustrated when they discover unexpected software on their computers. In some instances, the software application provides real value; in many instances the software may be considered "spyware." A lack of standards and definitions has made it difficult for consumers and businesses alike to determine what is "spyware" and what is legitimate software. Consequently, the promise of easy-to-use and valuable consumer downloadable software has been severely hindered by a lack of trust.

TRUSTe Oversight

TRUSTe, the leading online privacy certification organization, has partnered with major online consumer portals and other industry leaders to develop standards and a certification program for downloadable applications.

TRUSTe, with its program sponsors, determined the following objectives

- Noticeably improve the consumer experience with downloadable applications
- Establish first industry-wide standards for developers of downloadable applications
- Identify and elevate trustworthy applications for distributors and marketers
- Protect the valued brands of online advertisers by enabling them to know which applications are trustworthy and which are not.

The Trusted Download Program certification combines strict standards, thorough review, ongoing monitoring, enforcement mechanisms and powerful market incentives.

The Program is currently in Beta and will elevate those applications that meet the certification requirements through a whitelist, thereby providing consumer portals and other businesses a tool to distinguish responsible software applications. For downloadable software developers, the program will provide guidance on responsible behavior. Consumers will see that certified downloadable applications provide improved disclosures, more explicit control mechanisms, easier uninstall, and more respect

autres entreprises un outil leur permettant de discerner les applications dignes de confiance. En ce qui concerne les développeurs d'applications téléchargeables, le Programme sera leur guide vers un comportement responsable. Les consommateurs constateront que les applications téléchargeables homologuées fournissent une meilleure protection en matière de communication, des mécanismes de contrôle plus clairs, une fonction de désinstallation plus facile à exécuter et qu'elles affichent un plus grand respect pour leurs données personnelles.

Essais en phase Bêta

La phase Bêta vise à inciter les concepteurs de logiciels à créer des applications fiables offrant à leurs partenaires et à leurs publicitaires potentiels une vision transparente de leurs pratiques. Pendant cette phase, TRUSTe travaillera avec des experts industriels et d'autres intervenants en vue d'affiner le processus d'homologation, les normes, les protocoles d'essais et les modèles de gestion.

Commanditaires du Programme de téléchargement fiable

AOL, C|net download.com, Computer Associates, Verizon, Yahoo!, Microsoft

Incitations à la conformité

TRUSTe fournira aux publicitaires, aux distributeurs, aux portails de consommateurs et aux autres parties intéressées une « liste blanche » d'applications homologuées. La liste blanche du Programme sera utilisée comme un outil pour aider les entreprises à décider quelles applications sont respectueuses et donc peuvent être utilisées à des fins publicitaires ou être proposées aux consommateurs comme un service. Les fournisseurs d'applications devront proposer un répertoire des publicités homologuées aux publicitaires qui souhaitent s'assurer que leurs publicités ne touchent que les utilisateurs ayant donné leur assentiment. À terme, TRUSTe établira un registre des annonceurs.

La liste blanche du Programme de téléchargement fiable offrira des incitations

for their personal information.

Beta Testing

The Beta period is designed to increase incentives for software designers to develop trusted applications by giving their potential business partners and advertisers transparency into their practices. During this period TRUSTe will be working with industry experts and others to refine the certification processes, standards, testing protocols and business models.

Trusted Download Sponsors

AOL, C|net download.com, Computer Associates, Verizon, Yahoo!, Microsoft

Incentives for Compliance

TRUSTe will serve a "whitelist" of certified applications to advertisers, distributors, consumer portals and other interested parties. The Program's whitelist will be used as a tool to help businesses decide which applications are respectful and therefore which applications can be used for advertising or that they can offer to consumers as a service. Application providers, must offer certified advertising inventory for advertisers who wish to ensure that their advertisements only reach users who have provided consent. At a later date, TRUSTe will establish an advertiser registry.

The Trusted Download Program whitelist will provide economic incentives for software providers to achieve certification. Certified applications will be more widely distributed in trusted networks, will receive a larger share of advertising expenditures, can charge premium pricing for certified inventory, and will be able to develop additional partnerships.

Scope

The program is aimed at consumer downloadable software applications. It does not cover software downloaded exclusively to handheld devices (i.e. mobile phones). While it focuses specific requirements on advertising and tracking software, many requirements also apply to all consumer downloadable applications. Advertising and tracking software providers will likely need to

économiques aux fournisseurs de logiciels pour qu'ils détiennent leur homologation. Les applications homologuées seront distribuées plus largement par des réseaux de confiance, elles recevront une part plus importante des dépenses publicitaires, elles se vendront au prix fort du fait de leur inscription au répertoire homologué et elles pourront susciter des partenariats supplémentaires.

Champ d'application

Le Programme vise les applications logicielles téléchargeables destinées aux consommateurs. Il ne concerne pas les logiciels téléchargeables uniquement sur les appareils portatifs (p. ex., les téléphones cellulaires). Alors que le Programme concentre ses exigences précises sur les logiciels publicitaires et les logiciels espions, un grand nombre des exigences s'appliqueront aussi aux applications téléchargeables. Les fournisseurs de logiciels publicitaires et espions devront changer leurs pratiques actuelles de manière significative pour obtenir leur homologation. De plus, le Programme fournira des normes visant toutes les applications afin d'offrir aux consommateurs une protection accrue en cas de communication de leurs renseignements personnels, une désinstallation plus facile et d'autres avantages.

Homologation

Les fournisseurs de logiciels soumettront à TRUSTe un contrat et un questionnaire dûment rempli comprenant des questions sur la manière dont leur application est distribuée. TRUSTe réalisera une évaluation approfondie des applications téléchargeables par rapport aux normes du Programme afin de s'assurer qu'elles ne contiennent pas d'activités interdites par le Programme. Une garantie supplémentaire de conformité sera fournie par une tierce partie, AppLabs, un laboratoire d'essai de logiciels qui évaluera les relais d'information et d'interaction de l'application avec le système d'exploitation du destinataire.

Éléments clés du Programme

Le Programme met en relief certaines exigences concernant tous les logiciels et détaille les exigences supplémentaires concernant les

significantly change current practices to earn certification. In addition, the program will provide standards for all applications to offer consumers enhanced disclosures, easier uninstall and other benefits.

Certification

Application providers will submit to TRUSTe a contract and a completed questionnaire including questions about how the application is distributed. TRUSTe will conduct a thorough evaluation of the downloadable applications against the program standards to ensure they do not involve activities that are prohibited by the Program. Additional compliance assurance will be provided by AppLabs, a third party software testing lab that will evaluate the application's relay of information and interaction with the recipient's operating system.

Key Program Elements

The Program outlines certain requirements for all software and specifies additional requirements for advertising and tracking software. This approach ensures that the Program addresses practices that historically have created consumer confusion and anxiety. However, all software will need to meet specific program requirements and will be tested for monitoring, relays, and behaviors that have historically been considered deceptive.

Notice

The Program imposes a layered approach, via a primary notice and reference notices such as the End User License Agreement, EULA, and the privacy statement. The primary notice must explain functionalities that impact the consumer experience and must be unavoidable, to ensure that users understand what they are downloading. EULAs and "opt-out" mechanisms are insufficient for providing such notice or obtaining consent. For example, unavoidable notice of any material changes to certain specified consumer settings is required for all software. Further, all ads delivered in certified advertising software must be labeled, and unavoidable notice of certain ad features must be provided.

Consent to Download is Required

Consumers must be offered notice and an opportunity to consent that is described in plain language and is as prominently displayed as the option to not download. Consent to download

logiciels publicitaires et les logiciels espions. Cette approche garantit que le Programme cible les pratiques qui, dans le passé, ont suscité la confusion et l'anxiété chez les consommateurs. Cependant, tous les logiciels devront se conformer aux exigences précises du Programme et seront vérifiés sur les plans de la surveillance, des relais et des comportements qui, par le passé, ont été considérés comme trompeurs.

Avertissement
Le Programme impose une approche par étapes, par le biais d'un avertissement préalable et d'avis de référence, comme le Contrat de licence utilisateur final (CLUF) ou la déclaration de confidentialité. L'avertissement préalable doit expliquer les fonctionnalités qui auront une influence sur l'expérience du consommateur et il est obligatoire; il garantit que les utilisateurs comprennent ce qu'ils téléchargent. Les CLUF et les mécanismes de refus ne peuvent remplacer cet avertissement ni tenir lieu de consentement. Par exemple, tout changement de matériel concernant certaines installations de consommateurs bien spéciales doit être obligatoirement accompagné d'un avertissement pour tous les logiciels. De plus, toutes les publicités délivrées par un logiciel de publicité homologué doivent être labellisées et certains dispositifs publicitaires doivent obligatoirement être accompagnés d'un avertissement.

Obligation du consentement au téléchargement
Il faut fournir aux consommateurs un avertissement préalable et un formulaire de consentement écrit en langage simple et aussi visible que la possibilité de ne pas télécharger. Le consentement au téléchargement ne doit pas s'obtenir par une option pré-sélectionnée. Les CLUF et les mécanismes de refus ne peuvent tenir lieu d'avertissement ni de consentement.

Désinstallation facile
Le mode d'emploi de la désinstallation doit être facile à trouver et à comprendre, et les méthodes de désinstallation doivent être disponibles là où les consommateurs ont l'habitude de les trouver, par exemple dans la fonction « Ajouter/supprimer des programmes » du panneau de configuration de Windows. La désinstallation doit supprimer tous les logiciels associés à l'application désinstallée, et ne peut pas être conditionnelle à la fourniture de renseignements personnels, à moins que cette information ne soit nécessaire à la vérification du compte utilisateur.

may not be obtained with a pre-selected option. EULAs and "opt-out" mechanisms are insufficient for providing notice and obtaining consent.

Easy Uninstall
Instructions for uninstallation must be easy to find and easy to understand, and methods for uninstalling must be available in places where consumers are accustomed to finding them, such as the Add/Remove Programs feature in the Windows Control Panel. Uninstallation must remove all software associated with the particular application being uninstalled, and cannot be contingent on a consumer's providing Personally Identifiable Information, unless that information is required for account verification.

Prohibited Activities
No company can have an application certified if any of its applications exhibits a behavior listed in the Program's Prohibited Activities section.

Examples of prohibited activities include:
- Taking control of a consumer's computer
- Modifying security or other settings of the computer to cause damage or harm
- Spyware tactics for surveillance and tracking, such as keystroke logging
- Preventing reasonable efforts to block installation or to uninstall
- Allowing a certified application to be bundled with any application currently engaging in any of the prohibited activities

Special Protections for Children
Companies in the Program must prevent the distribution of their advertising or tracking software on children's websites—including by prohibiting their distribution partners and affiliates from such distribution.

Affiliate Controls
Since many advertising and tracking applications are distributed through second and third-party affiliates and/or bundled with other programs, relationships must be disclosed in attestations. Certified software is subject to random testing on instances found wherever an individual might encounter them.

Prior Behavior
The Program includes provisional certification for companies that have previously engaged prohibited activities. In order to be certified, these companies will be subject to additional oversight

Activités interdites
Une entreprise ne pourra obtenir aucune homologation si l'un de ses logiciels présente un comportement figurant dans la section des activités interdites par le Programme.

Exemples d'activités interdites
- Prendre le contrôle de l'ordinateur d'un consommateur.
- Modifier la sécurité ou les autres paramètres de l'ordinateur pour l'endommager.
- Utiliser des tactiques d'espionnage comme la reconnaissance de la frappe pour surveiller et poursuivre le consommateur.
- Empêcher les efforts raisonnables de blocage d'installation ou de désinstallation.
- Permettre qu'une application homologuée soit livrée avec toute application pratiquant une ou des activités interdites.

Protection visant particulièrement les enfants
Les entreprises inscrites au Programme doivent empêcher la distribution de leur publicité ou de leurs logiciels espions sur les sites Web destinés aux enfants, y compris en interdisant cette distribution à leurs partenaires [de distribution] et à leurs sociétés affiliées.

Contrôle des sociétés affiliées
Dans la mesure où les applications publicitaires ou espionnes sont distribuées par le biais de sociétés affiliées, directement ou indirectement, ou livrées avec d'autres programmes, leurs relations doivent être indiquées dans les attestations. Les logiciels homologués sont soumis à des tests aléatoires sur des situations auxquelles un utilisateur pourrait être confronté.

Comportement antérieur
Le Programme comporte une homologation provisoire pour les entreprises ayant pratiqué par le passé des activités interdites. Afin d'obtenir leur homologation, ces entreprises seront soumises à une surveillance supplémentaire comprenant un contrôle renforcé et une obligation de reprendre contact avec tous les utilisateurs ayant téléchargé une version non homologuée de leur logiciel afin d'obtenir leur accord.

Répertoire de publicités sélectionnées
Les entreprises inscrites au Programme doivent maintenir à jour un répertoire de publicités distinguant les versions homologuées des non homologuées. Le fournisseur d'applications doit pouvoir offrir de la publicité aux utilisateurs ayant

including enhanced monitoring and a requirement to go back to all users who downloaded an uncertified version of the software application and obtain their opt-in consent.

Segregated Ad Inventory
Companies in the Program must maintain segregated ad inventory in certified versus uncertified applications. The application provider must be able to serve ads to users from whom consent was obtained versus users from whom consent has not been acceptably obtained.

Monitoring
Certified applications are monitored by TRUSTe for ongoing compliance with the Program's strict standards. A company risks termination from the program if any one of its certified applications violates the standards.

Enforcement
If monitoring uncovers suspected non-compliance, an application, or in some cases all of a company's applications, will be subjected to enforcement procedures by TRUSTe. Depending on severity and the results of a TRUSTe investigation, an application may be suspended or removed from the program whitelist. In certain cases, a company or application may be terminated from the Program and the fact of its termination made public.

TRUSTe

TRUSTe® is an independent, nonprofit organization that promotes and enables trust based on privacy, transparency and the establishment of best practice standards for organizations conducting business on the internet. We certify and monitor web site privacy and email policies, monitor practices, and resolve thousands of consumer privacy problems every year. For the Trusted Download Certification Beta Program, TRUSTe's expertise in enforcing best practices in consumer notice and choice is complemented by AppLabs, a software-testing lab, which will handle the technical testing and monitoring of certified applications.

donné leur consentement mais pas à ceux dont le consentement volontaire n'a pu être recueilli.

Surveillance
Les applications homologuées sont surveillées par TRUSTe qui en garantit en permanence la conformité aux normes rigoureuses du Programme. Une entreprise risque la radiation du Programme si l'une de ses applications homologuées entre en violation avec les normes.

Application
Si la surveillance révèle un cas possible de non-conformité, une application ou, dans certains cas, toutes les applications de l'entreprise, seront soumises à des procédures d'exécution par TRUSTe. En fonction de la gravité des faits et des résultats de l'enquête de TRUSTe, une application pourra être suspendue ou retirée de la liste blanche du Programme. Dans certains cas, une entreprise ou une application pourra être radiée du Programme et cette radiation sera rendue publique.

TRUSTe

TRUSTe® est un organisme indépendant à but non lucratif qui encourage et facilite la confiance sur la base de la protection des données personnelles, de la transparence et de l'établissement de normes de bonne pratique pour les entreprises ayant une activité commerciale sur Internet. TRUSTe homologue et surveille les pratiques de protection des données personnelles sur les sites Web et la politique concernant le courrier électronique. TRUSTe règle chaque année des milliers de litiges concernant la protection des données personnelles. En ce qui concerne le Programme de téléchargement fiable en phase Bêta, l'expertise de TRUSTe pour faire appliquer les bonnes pratiques dans les avertissements aux consommateurs et leur prise de décision est complétée par AppLabs, un laboratoire d'essai de logiciels, qui prendra en charge les essais techniques et la surveillance des applications homologuées.

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Qu'est-ce que le Cadre de règles refuges sur les fichiers nominatifs (« Safe Harbour Framework ») conclu entre l'Union européenne et les Etats-Unis ?

What is the EU-US Safe Harbour Framework?

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Qu'est-ce que le Cadre de règles refuges sur les fichiers nominatifs («Safe Harbour Framework») conclu entre l'Union européenne et les États-Unis?

TRUSTe peut aider les entreprises faisant des affaires avec des citoyens européens à faire homologuer leur conformité à la Directive européenne concernant la protection des données. La Directive interdit le transfert de données à caractère personnel de citoyens européens vers des pays non membres de l'Union européenne (UE) ne garantissant pas un niveau adéquat de protection des données personnelles. Le département américain du Commerce, de concert avec la Commission européenne, a élaboré un Cadre de règles refuges sur les fichiers nominatifs (« Safe Harbor Framework ») qui permet aux organisations américaines de se conformer à la Directive en se soumettant au faisceau des Règles refuges sur la protection des données personnelles (« Safe Harbor Privacy Principles »). Les entreprises font certifier leur conformité à ces règles sur le site Web du département américain du Commerce. Le Cadre a été adopté par l'Union européenne en 2000 et garantit aux entreprises qui se soumettent aux Règles refuges que l'Union Européenne reconnaîtra à leurs pratiques un niveau adéquat de protection des données personnelles des citoyens européens.

Pourquoi un label TRUSTe – Cadre de règles refuges de l'UE?

Le programme de labellisation de TRUSTe vérifie la conformité des entreprises avec le Cadre de règles refuges sur les fichiers nominatifs (« Safe Harbour Framework »), propose une possibilité différente de règlement des litiges et aide votre organisation à se préparer à l'auto-homologation auprès du département américain du Commerce. Afficher le label TRUSTe est une manière de montrer aux consommateurs du monde entier que les entreprises prennent au sérieux la protection de leurs données personnelles.

Quels sont les avantages?

Rationalisation de la conformité légale au Cadre de règles refuges sur les fichiers nominatifs :

- vérification de la conformité aux

What is the EU-US Safe Harbor Framework?

If you do business with European citizens, TRUSTe can help you certify your compliance with the EU Directive on Data Protection. The Directive prohibits the transfer of European cititzens' personal data to non-European Union nations that do not meet the EU's "adequacy" standard for privacy protection. The U.S. Department of Commerce, in concert with the European Commission, developed a "Safe Harbor Framework" that allows US organizations to comply with the Directive by abiding by a set of Safe Harbor Privacy Principles. Companies certify their compliance with these Principles on the U.S. Department of Commerce Web site. The Framework was approved by the EU in 2000 and gives companies that abide by the Principles assurance that the EU will consider their practices "adequate" privacy protections for EU citizens.

Why TRUSTe's EU Safe Harbor seal?

The TRUSTe EU Safe Harbor Seal Program verifies your compliance with the Safe Harbor Framework, includes alternative dispute resolution, and helps your organization get ready for self-certification with the U.S. Department of Commerce. Displaying the TRUSTe EU Safe Harbor seal signals to consumers around the globe that you take their privacy seriously.

What are the Benefits?

Streamline legal compliance with the EU safe harbor framework

- Verifies compliance with the Safe Harbor Privacy Principles
- Provides dispute resolution of consumer complaints about data Collected online or offline, as required for Safe Harbor status

Prepares you for self-certification with the U.S. Department of Commerce.

Builds trust and confidence

- Brands your organization and Web site as EU-US Safe Harbor compliant by posting the distinctive EU Safe Harbor seal
- Third-party certification emphasizes

Règles refuges sur la protection des données personnelles
- règlement des litiges à propos de plaintes de consommateurs sur la collecte de données en ligne ou hors connexion, comme le requiert le label des règles refuges

Préparation à l'auto-homologation auprès du département américain du Commerce.

Constitution d'un climat de confiance :
- présentation de votre organisation et de votre site Web comme conformes au Cadre de règles refuges de fichiers nominatifs de l'UE et des États-Unis en arborant le label des règles refuges de l'UE
- homologation par une tierce partie qui souligne l'engagement de votre organisation en faveur de la protection des données personnelles et du choix du consommateur.

« Il est essentiel que nous nous conformions au cadre de règles refuges sur les fichiers nominatifs lorsque nous traitons avec des clients européens. L'affichage du *label* TRUSTe UE prouve notre conformité avec le cadre européen et montre que nous prenons au sérieux le traitement des données des consommateurs. Cela facilite la vente de nos services. » David Stark, Agent de la protection de la vie privée, SRT

Caractéristiques de TRUSTe

Processus d'homologation de TRUSTe
Les candidats complètent une auto-évaluation décrivant leur manière de recueillir, d'utiliser et de traiter les informations. Les gestionnaires de clientèle comparent toutes ces évaluations aux procédures réellement suivies et aux divulgations réellement faites sur le site Web grâce à un examen général du site. Les candidats reçoivent un rapport détaillé des constatations, qui donne les résultats de l'examen général et établit la liste des actions à mener pour se mettre en conformité avec les normes du Programme.

Labels TRUSTe
À la suite de leur homologation, les membres reçoivent des labels TRUSTe identifiant les sites sécurisés, à afficher sur leurs pages Web. Les

your organization's commitment to privacy and consumer choice

"It is critical that we abide by the safe harbor framework when dealing with business customers in Europe. Our display of TRUSTe's EU Seal marks our compliance with the EU framework and shows that we take customer data handling seriously. It makes selling our services that much easier."
David Stark, Privacy Officer
North America, TNS

TRUSTe Features

TRUSTe certification process
Applicants complete a self-assessment detailing information collection, use, and procedures. Client services managers review all self-assessments against actual Web site procedures and disclosures with a site walkthrough. Applicants receive a detailed site findings report which identifies the results of the site walkthrough and lists action items for the applicant to complete to become compliant with program standards.

TRUSTe seals
After passing the certification process, members receive TRUSTe's trusted web seals to display throughout their respective web pages. Client services managers provide seal placement guidance to ensure members are maximizing the impact of the seals. More than one million consumers click on these seals per month to confirm TRUSTe membership.

Monitoring and Scanning
TRUSTe uses a combination of tools including MAXAMINE scanning technology and personal attention to monitor licensed sites for breaches of their privacy policies. Compliance analysts look for things such as encryption measures on sensitive pages and undisclosed "cookies", or single-pixel tracking devices. Oftentimes, violations are unintentionally introduced when organizations update their pages, undergo changes in ownership, or launch new initiatives such as contests or newsletters.

Watchdog Dispute Resolution System
The TRUSTe Watchdog Dispute Resolution System is an online tool that allows consumers to report violations of posted privacy statements, or

gestionnaires de la clientèle aident les clients à placer au mieux les labels, pour maximiser leur impact. Plus d'un million de consommateurs cliquent chaque mois sur ces labels pour vérifier l'adhésion d'une entreprise à TRUSTe.

Surveillance et balayage
TRUSTe utilise un ensemble d'outils, dont la technologie de balayage MAXAMINE et sa propre vigilance, pour surveiller les sites homologués et détecter les failles dans leur politique de confidentialité. TRUSTe recherche par exemple les mesures de cryptage des pages au contenu délicat et les témoins de connexion cachés ou les dispositifs de repérage à pixel unique. Il arrive souvent que des irrégularités surviennent par accident, lorsque les organisations mettent leur site à jour, changent de propriétaire ou lancent de nouvelles activités comme un concours ou un bulletin d'information.

Procédure de surveillance pour la résolution des litiges
La procédure de surveillance de TRUSTe pour la résolution des litiges est un outil en ligne qui permet aux consommateurs de signaler les infractions aux règles affichées de protection des données personnelles ou les sujets d'inquiétude particuliers sur la protection des données personnelles, visant les sites Web membres de TRUSTe.

Protection du label
Pour préserver la volonté des entreprises sous licence TRUSTe de se conformer à des normes strictes et pour garantir la conformité constante à ces normes, TRUSTe protège vigoureusement ses labels. TRUSTe conserve une « liste noire » des sites Web usurpant le label sur son site Web TRUSTe.org.

Le processus TRUSTe

1 L'organisation complète un contrat TRUSTe et une auto-évaluation.

2 TRUSTe effectue un premier examen du site et donne une série de recommandations écrites sous forme de rapport détaillé des constatations.

3 L'entreprise met en œuvre les recommandations sur son site.

specific privacy concerns pertaining to TRUSTe member Web sites.

Trademark Enforcement
To protect the investment of TRUSTe licensees to meet strict standards, and to ensure ongoing compliance, TRUSTe vigorously enforces trademarks. TRUSTe maintains a "blacklist" of trademark violator Web sites on the TRUSTe.org Web site.

The TRUSTe Process

1 your organization fills out a TRUSTe contract and self-assessment.

2 TRUSTe conducts an initial site walkthrough and provides a set of written recommendations in the form of a site findings report.

3 you implement recommendations on your website.

4 TRUSTe awards you privacy seals. Display these where you collect information to build confidence with customers.

5 TRUSTe ensures ongoing compliance and monitoring with MAXAMINE scanning and the TRUSTe watchdog Dispute resolution system.

4 TRUSTe décerne à l'entreprise des labels de protection de la vie privée. Ceux-ci doivent être affichés sur les pages où l'information est recueillie pour que le consommateur se sente en confiance.

5. TRUSte garantit une conformité et une surveillance par balayage constantes ainsi que la fourniture de la Procédure de surveillance pour la résolution des litiges.

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

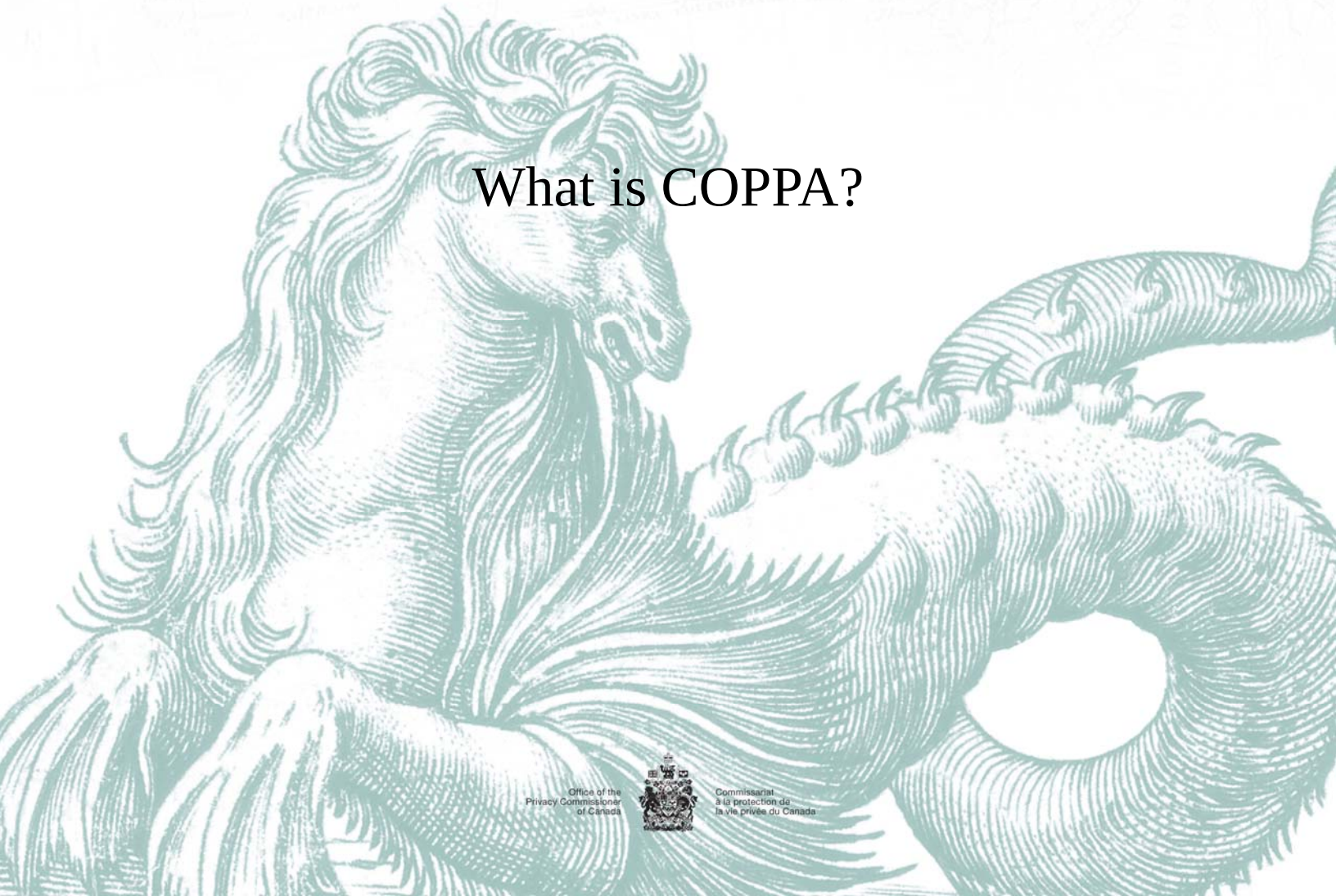
TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Qu’est-ce que la COPPA ?

What is COPPA?



Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Qu'est-ce que la COPPA?

La loi dénommée Children's Online Privacy Protection Act (COPPA, *Loi sur la protection des enfants en ligne*) réglemente la collecte en ligne des données à caractère personnel auprès d'enfants de moins de 13 ans. Son objectif principal est de fournir aux parents un moyen de contrôler le type d'informations recueillies en ligne auprès de leurs enfants, et la façon dont ces informations sont utilisées. La Loi s'applique aux exploitants de sites Web et de services en ligne destinés aux enfants de moins de 13 ans, et aux sites visant un public plus général qui recueillent des données à caractère personnel auprès d'enfants de moins de 13 ans.

Pourquoi un label TRUSTe pour les enfants?

La Federal Trade Commission a reconnu que TRUSTe était un organisme conforme au Programme des règles refuges de la COPPA. Le label TRUSTe pour les enfants atteste le fait qu'une entreprise est en conformité avec la COPPA – et donc fait savoir aux parents que les données personnelles de leurs enfants sont en sécurité.

Le label TRUSTe pour les enfants s'applique en particulier aux sites Web qui sont partiellement ou totalement destinés aux enfants de moins de 13 ans et aux sites visant un public plus général qui recueillent des données à caractère personnel auprès d'enfants de moins de 13 ans. Les détenteurs du label pour les enfants se soumettent également aux exigences du label de protection des données personnelles en ligne, qui comprend une surveillance permanente du site et un autre mode de règlement des litiges.

Quels sont les avantages?

Conformité aux règles de la COPPA :

- Rationalisation de la conformité aux règles de la COPPA en intégrant une règle refuge attestée.
- Prestation d'un autre mode de règlement des plaintes concernant la protection des données personnelles.
- Conformité constante pendant toute l'année grâce aux outils de balayage et à la présélection du courrier électronique.

Établissement d'un climat de confiance

What is COPPA?

The Children's Online Privacy Protection Act (COPPA) Rule regulates the online collection of personal information from children under 13 years of age. The primary goal of the COPPA Rule is to give parents control over what information is collected from their children online and how such information may be used. The Rule applies to operators of Web sites and online services directed to children under 13, and to general audience Web sites that knowingly collect personal information from children under 13.

Why TRUSTe's Children's Seal?

The Federal Trade Commission has approved TRUSTe as a COPPA Safe Harbor program. The TRUSTe Children's Seal certifies that your business is compliant with the COPPA Rule – letting parents know that their kids' information is safe.

The TRUSTe Children's Seal specifically applies to Web sites that are fully or partially targeted towards children under the age of 13, and to general audience Web sites that knowingly collect personal information from children under 13. Children's seal holders also abide by the requirements of TRUSTe's standard Web Privacy Seal Program, including ongoing site monitoring and alternative dispute resolution.

What are the benefits?

COPPA compliance

- Streamlines legal compliance with COPPA by joining an approved Safe Harbor
- Provides alternative dispute resolution for privacy complaints
- Keeps you compliant throughout the year with scanning tools and email seeding

Builds trust and confidence

- Brands your organization and Web site as "child-friendly" by posting the distinctive TRUSTe Children's Seal
- Gives you and your customers access to consumer education pieces including Online Privacy: A Tutorial for Parents and Teachers
- Third-party approval emphasizes your organization's COPPA compliance and commitment to privacy and parental choice

- Mise en valeur des organisations « amies des enfants » et de leur site Web par l'apposition du label TRUSTe pour les enfants.
- Accès aux entreprises et à leurs clients à des documents d'éducation des consommateurs, y compris le guide *Online Privacy: A Tutorial for Parents and Teachers*.
- Homologation par une tierce partie, qui souligne la conformité à la COPPA et l'engagement des entreprises à l'égard de la protection des données personnelles et du choix parental.

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

EuroPrise
Sceau européen de protection de la vie privée

EuroPrise
European Privacy Seal

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Le projet du Sceau européen de protection de la vie privée appelé EuroPriSe (European Privacy Seal) permettra à des tiers d'attester que les produits de la TI et les services axés sur la TI sont conformes à la réglementation européenne en matière de protection de la vie privée et de sécurité des données.

EuroPriSe, le projet du Sceau européen de protection de la vie privée, vise à établir un mode de vérification de la conformité des produits de TI et des services axés sur la TI à la réglementation européenne concernant la protection de la vie privée et la sécurité des données à la fin d'une procédure en deux étapes : une évaluation du produit ou du service par des experts juridiques et de la TI, et une vérification par recoupement du rapport de vérification par un organisme de certification accrédité.

Un des principaux problèmes qui se posent à la société de l'information est le manque de confiance vis-à-vis les produits et les services de la TI en raison des possibilités d'une surveillance électronique. Les particuliers et les entreprises ont souvent besoin d'une « bonne dose de confiance » lorsqu'ils utilisent des produits et des services de TI qui se rapportent à la protection de la vie privée. À l'heure actuelle, il n'existe pas de lignes directrices transparentes concernant le choix d'un produit conforme à la sécurité des données et à la protection de la vie privée.

EuroPriSe fournira une procédure transparente et des critères fiables pour attribuer un sceau européen de protection de la vie privée. Ce sceau permet de s'assurer visuellement qu'un produit a été vérifié et approuvé par une organisation indépendante de protection de la vie privée, et d'indiquer qu'il s'agit d'un produit sécuritaire. De même, ce sceau de protection avantage les consommateurs et leur inspire confiance, et encourage les fabricants et les fournisseurs à commercialiser des biens et des services qui sont conformes à la protection de la vie privée.

EuroPriSe vise à établir ce qui suit :

- Certification volontaire du respect de la vie privée valide à l'échelle de l'Europe
- Procédure simple et transparente, et critères fiables
- Supervision par un tiers indépendant
- Attestation visible du respect de la vie privée

The European Privacy Seal (EuroPriSe) project will provide a trans-European privacy seal issued by independent third parties certifying compliance of ITproducts and IT-based services with European regulations on privacy and data security.

EuroPriSe, the European Privacy Seal project aims to establish a European product audit certifying compliance of IT-products and IT-based services with European regulations on privacy and data security after the completion of a specific two-step procedure: an evaluation of the product or service by accepted legal and IT experts and a crosschecking of the evaluation report by an accredited certification body.

One of the main problems facing the information society is a lack of trust in IT products and services caused by the possibilities of electronic surveillance. Citizens and business often need "a good faith belief" when using privacy relevant IT products and services. Currently there is no transparent guidance for choosing a data security and privacy compliant product.

EuroPriSe will provide a transparent procedure and reliable criteria to award a European Privacy Seal. The privacy seal visualizes that a product has been checked and approved by an independent privacy organisation and thus indicates a trustworthy product. Thus, the privacy seal at the same time fosters consumer protection and trust and provides a marketing incentive to manufacturers and vendors for privacy relevant goods and services.

EuroPriSe aims to establish

- Voluntary privacy certification valid throughout Europe
- Transparent non-bureaucratic procedure and reliable criteria
- Supervision by an independent third party
- Visibility of privacy compliance available for marketing
- Comparability of products by short public reports

The **EuroPriSe** project will adapt the successful certification scheme and criteria of the privacy seal (Guetesiegel) of the German state of Schleswig-Holstein to European requirements. **EuroPriSe** is addressed to manufactures of IT products and services related to processing or storage of personal data, to technical and legal IT

disponible pour la commercialisation
- Possibilité de comparer des produits grâce à de courts rapports publics

Le projet **EuroPriSe** adaptera aux exigences européennes la méthode éprouvée et les critères de certification (Guetesiegel) utilisés par l'État allemand de Schleswig-Holstein. **EuroPriSe** s'adresse aux entreprises de produits et de services de TI dans le domaine du traitement ou du stockage de données personnelles, aux experts techniques et juridiques de la TI, ainsi qu'aux autorités responsables de la protection des données intéressées à participer aux essais pilotes. Dans le cadre du projet, un atelier sera offert aux experts potentiels. On prévoit accorder les premiers sceaux européens de protection de la vie privée aux produits et aux services qui pourront être offerts en conformité avec la réglementation européenne en matière de protection de la vie privée et de sécurité des données.

Le consortium **EuroPriSe** est dirigé par le Centre indépendant de protection de la vie privée du Schleswig-Holstein (ICPP/ULD), en Allemagne. Les partenaires de huit pays d'Europe comprennent les autorités responsables de la protection des données, l'organisme de protection des données de Madrid, en Espagne, la Commission Nationale de l'Informatique et de Libertés (CNIL), en France, l'Académie autrichienne des sciences, en Autriche, la London Metropolitan University, au Royaume-Uni, la Borking Consultancy, aux Pays-Bas, la Ernst and Young AB, en Suède, la TÜV Informationstechnik GmbH, en Allemagne et la VaF s.r.o., en Slovaquie.

Financement par l'UE	1 234 000 €
Durée	De juin 2007 à novembre 2008
Site Web	www.european-privacy-seal.eu
Contact	Kirsten Bock, europrise@datenschutzzentrum.de
Pays participants	Autriche, France, Allemagne, Slovaquie, Espagne, Suède, Pays-Bas, Royaume-Uni

experts and to data protection authorities interested in participating in the pilot trials. The project will conduct a workshop for potential experts and plans to award the first European Privacy Seals to products or services that can be deployed in compliance with European regulations on privacy and data security.

The **EuroPriSe** consortium is lead by the Independent Centre for Privacy Protection Schleswig-Holstein (ICPP/ULD), Germany. The partners from 8 European countries include the data protection authorities from Madrid, Agencia de Protección de Datos de la Communidad de Madrid and France, the Commission Nationale de l'Informatique et de Libertés (CNIL), the Austrian Academy of Science and London Metropolitan University from the UK, Borking Consultancy from the Netherlands, Ernst and Young AB from Sweden, TÜV Informationstechnik GmbH from Germany, and VaF s.r.o. from Slovakia.

EU Funding	1 234 000 €
Duration	June 2007 — November 2008
Website	www.european-privacy-seal.eu
Contact	Kirsten Bock, europrise@datenschutzzentrum.de
Participating Countries	Austria, France, Germany, Slovakia, Spain, Netherlands, United Kingdom