



# Privacy Guidelines: Assessing your Privacy Architecture

## Introduction

Did you know that 71 percent of consumers look for online trustmarks before doing business online?<sup>1</sup> Or did you know that 73 percent of consumers have refused to give information to a Web site because they felt it was too personal or unnecessary?<sup>2</sup> Information is the new online currency and your success in this online information marketplace depends on the level of trust you have with individuals visiting your Web site.

There may be no quicker way to lose customer trust than by failing to adequately advertise your privacy practices to prospective customers or by failing to communicate with established customers when you make significant privacy changes to your site's operation. The costs of failure are high: in addition to lost revenue and reputational damage, companies that fail to respect the privacy of their customers can also face legal ramifications.

Protecting customer privacy goes beyond securing your network from hackers and posting a boilerplate privacy policy. Protecting customer privacy requires the development of a robust plan, unique to your company, which minimizes data collection, adequately secures collected data, and effectively communicates privacy practices to customers.

Moreover, your plan must be adaptable: it should be reviewed frequently and evolve with your business and the greater marketplace. New technologies and practices will raise new privacy questions that you must answer. Do you use behavioral advertising to target potential customers? Do you collect biometric information (e.g., fingerprints, retinal scans)? Does your company use cloud computing to store data? While you may answer "no" to these questions today, the answer may be "yes" to these, and many new questions, tomorrow.

The guide that follows provides a framework to assess your company's privacy practices and needs.

---

## Navigating the Whitepaper

1. Who do you collect information from?
2. How do you use the data you collect?
3. What data do you collect?
4. How do you collect data?
5. How do you store the data you collect?
6. Do you have a security breach response plan?
7. How do you market your business?
8. Do you adequately communicate your privacy practices?
9. Data Collection for the Future
10. Conclusion
11. TRUSTe Privacy Assessment Checklist
12. TRUSTe Solutions

1 "Trust Marks: What's Behind the Label Counts". Yankee Group. 2009. <http://us.mcafee.com/en-us/local/docs/LR-51384.pdf>

2 "Future of Privacy Forum Online Behavioral Advertising "Icon" Study". January 25, 2010. [http://futureofprivacy.org/final\\_report.pdf](http://futureofprivacy.org/final_report.pdf)

## 1. Who do you collect information from?

*The sources of the data you receive may determine many of your privacy obligations.*

### Questions to consider:

- ➔ Do you receive information about your customers from third parties?
  - Your business may require you to obtain customer information from third parties such as credit reporting agencies, banks, and other sources which may subject you to privacy laws and obligations. For example, if you access consumer credit reports you may be subject to the Fair Credit Reporting Act. You may also be subject to contractual privacy and security obligations such as those set forth by the payment card industry (e.g., the Payment Card Industry Data Security Standard) or if you act as a vendor or supplier to another business.
- ➔ Which states are your customers from?
  - State law may apply to your company based on the geographic location of your customers. These state laws may impose obligations related to data breach notification, storage of information, and security measures. Nevada and Massachusetts are two prominent examples of state privacy mandates that go beyond basic data breach notification laws.
- ➔ Do you collect information from people outside of the U.S.?
  - Foreign data protection laws, especially those in Europe, impose different requirements than U.S. laws. The U.S. Department of Commerce administers a Safe Harbor Program that can guide foreign compliance efforts. Learn about [TRUSTe's EU Safe Harbor Privacy Program](#).
- ➔ Do you collect information from children?
  - The Children's Online Privacy Protection Act (COPPA) is a federal law governing the collection and use of information from children under 13. You may be required to obtain parental consent depending on the information you are collecting. Learn about [TRUSTe's Children's Privacy Program](#).

## 2. How do you use the data you collect?

*Companies should be transparent (and cannot be misleading) about what they do with the customer information they collect. Customers want to know how you use their data and recent privacy incidents at major national companies have shown they will push back if they feel a company is not making adequate disclosures.*

### Questions to consider:

- ➔ Do you use collected data solely for transactional purposes or do you use for marketing, as well?
  - Companies must be clear with consumers about what is done with the information collected. Frequently, companies will give customers the ability to opt-in to having their information used for marketing purposes.
- ➔ Do you share information with third parties for the purposes of processing transactions?
  - Sharing consumer information with any party, whether for marketing or transactional purposes, should be disclosed to consumers.

### ➔ Do you sell customer information to third parties?

- As with all data collection, companies should be upfront with consumers when information collected by the company is sold to third parties whether that information is names and addresses sold to direct marketers or, for example, an Internet Service Provider selling aggregate information about web surfing habits. Several laws regulate the sharing of information with third parties by financial institutions.

## 3. What data do you collect?

*Your privacy obligations may be further defined by the type of information you collect. One of the best ways to minimize your privacy exposure is to limit the amount of data you collect to only that which is necessary to conduct the business transaction. This is especially true with regard to so-called “sensitive information” such as a Social Security numbers, medical information, and financial information (e.g., credit or debit card numbers or other financial account numbers).*

### Questions to consider:

#### ➔ Do you collect financial information?

- If you collect credit card or bank account numbers to complete your transactions you may be subject to contractual privacy obligations with payment card brands and banks. There are also rules regarding the form in which credit card information is printed on receipts. If you extend credit to customers or are a financial institution you may be subject to the FTC’s Red Flags Rule, which is designed to curb identity theft.
- The Gramm-Leach-Bliley Act (GLBA) sets forth privacy obligations for “financial institutions.” A financial institution is more than just a bank and includes companies that may not traditionally be thought of as financial institutions, such as tax preparers and real estate settlement services. Certain provisions of the GLBA apply to anyone who receives nonpublic personal information from a financial institution.

#### ➔ Do you collect health information?

- The Health Information Portability and Accountability Act (HIPAA) sets forth privacy requirements for “covered entities” including health care providers, health plans, and health care clearinghouses. Companies that work with covered entities may be contractually obligated to comply with HIPAA. Companies that are not covered by HIPAA but are involved with electronic health records are subject to privacy requirements under the American Recovery and Reinvestment Act.

#### ➔ Do you access consumer reports?

- If you access consumer reports, such as credit reports, you may be subject to the requirements of the Fair Credit Reporting Act.

## 4. How do you collect data?

*Data provided directly by the customer is only one way that businesses collect data. Online companies may also use automatic data collection tools. It is a best practice to provide customers with a complete and meaningful explanation of the automatic data tools you use, what information is collected through those tools, and how that information is used.*

### Questions to consider:

- ➔ Do you use cookies to collect data?
  - Cookies are small text files that are stored on a Web site visitor's computer. The file stores and transmits information regarding the visitor, such as log-in information and pages visited. Privacy concerns arise with regard to how long a cookie remains on a visitor's computer, what information is collected, and who is placing the cookie on the visitor's computer (e.g., third party advertisers). You should consider what, if any, types of cookies you are using (e.g., session cookies, persistent cookies, Flash cookies) and whether other parties may be using your Web site to place cookies.
- ➔ Do you use web beacons to collect data?
  - A web beacon is a small, transparent graphic embedded on a web page or in an email that is downloaded when a visitor accesses a web page or opens an email. Like cookies, web beacons allow companies to monitor visitor activity and collect visitor information.
  - Network Advertising Initiative [guidance on use of web beacons](#), developed with assistance of TRUSTe
- ➔ Do you use embedded web links?
  - A company may use an embedded web link, for example, in an email to consumers to direct the consumer to a particular web page via the company's servers. This may allow the company to determine the effectiveness of marketing efforts. Privacy concerns may arise when the information collected is connected to an identifiable person.
  - Tools exist, for example, that allow a company to recreate a visitor's web session. It is important to remain current on new tools as well as the privacy implications of those technologies.

## 5. How do you store the data you collect?

*Adequate security is fundamental to protecting customer privacy. Remember that a complete security program protects data from outside threats as well as threats, intentional and unintentional, from within. There are several steps in assessing whether you are storing data in a way that minimizes the risk of a privacy violation.*

### Questions to consider:

- ➔ Where do you store the data?
  - Is it on servers, on portable media (such as thumb drives), laptops, and cell phones? Are employees accessing data from home? Who has access to the data?
  - Are all of your employees able to access data or is sensitive data limited to the fewest number of employees necessary to complete a transaction? Are you training employees on proper handling of sensitive data? Companies may be held liable for employee misuse of sensitive data if the company is not exercising due diligence.
- ➔ Who has access to the data?
  - Are all of your employees able to access data or is sensitive data limited to the fewest number of employees necessary to complete a transaction? Are you training employees on proper handling of sensitive data? Companies may be held liable for employee misuse of sensitive data if the company is not exercising due diligence.

- ➔ How long are you retain the data?
  - Sensitive data should be kept for as long as there is a legitimate business need and no longer.
- ➔ Do you encrypt the data?
  - Encryption of sensitive information is now the law in some states for any company involved in commerce.
- ➔ Do you appropriately secure electronic and physical data?
  - **View TRUSTe's Security Guidelines.**
  - At least one state (Massachusetts) requires companies to have a written information security program in place. Note that PCI DSS may not be sufficient to secure data without further measures. Are you taking appropriate physical security measures in addition to electronic security measures – e.g., locked file cabinets, appropriate building security?
- ➔ How do you delete data?
  - Paper documents containing sensitive information should be shredded and laptops and portable media should be wiped clean. If you use credit reports, you may be subject to the Federal Trade Commission's Disposal Rule.
- ➔ Does your forecast call for clouds?
  - Businesses and individuals are increasingly using third party infrastructures for data storage. While so-called "cloud computing" can be financially beneficial for companies, it raises privacy questions about who can access and monitor the stored data

## 6. Do you have a security breach response plan?

*A data security breach is an emergency situation. There will not be time to determine roles and responsibilities within your company or the legal and contractual obligations you may have. Your company should have a plan in place to detect and address threats promptly. The plan should address the questions in this section.*

### Questions to consider:

- ➔ Who within the company should be contacted immediately to avoid further data loss?
  - This should include those with the authority to make decisions for the company as well as those with the technical expertise required to execute those decisions.
- ➔ What physical steps should be taken to avoid further data loss?
  - Consider, for example, how compromised equipment may need to be disconnected.
- ➔ How will the security incident be investigated?
  - Your plan should identify, among other things, who will lead the immediate investigation and how you will determine if there is a violation of federal or state law.
- ➔ What are your notification requirements?
  - A breach may trigger state or federal law. For example, almost every state has a breach notification law requiring notice to consumers, and sometimes law enforcement, in the event that certain information is accessed or acquired. You may have additional contractual notification requirements.

## 7. How do you market your business?

*Successful marketing is key to a successful business but there are an increasing number of privacy issues related to marketing that must be considered. When assessing privacy and marketing think both of how you communicate with customers as well as how you identify potential customers.*

### Questions to consider:

- ➔ Are you compliant with state and federal marketing laws?
  - CAN-SPAM is the federal law regulating commercial e-mail. It applies to all commercial mail including business-to-business email. Non-compliance can be costly: each separate email in violation is subject to penalties of up to \$16,000. Learn about [TRUSTe's Email Privacy Program](#).
- ➔ Are you using behavioral advertising to target specific consumers?
  - Are you targeting ads to consumers based on web surfing history? If you are not collecting this data, are you receiving it from third party advertising networks? While behavioral advertising is not illegal, it is the subject of much debate and has been studied by the Federal Trade Commission. This area may apply to nonpersonally identifiable information such as IP address. Learn about [TRUSTe's Behavioral Advertising Notice and Choice Program](#)

## 8. Do you adequately communicate your privacy practices?

*Clearly and completely communicating your privacy practices to your customers is not only a best privacy practice but can also be an effective marketing tool. Skipping the legalese and minimizing the jargon can help customers understand that you respect their privacy and may make them more comfortable patronizing your business.*

### Questions to consider:

- ➔ Do you have a privacy policy?
  - It is not enough to have a boilerplate privacy policy. Your privacy policy should reflect your company. Review your policy frequently to ensure that it accurately and completely explains your practices. Be sure that your policy does not over-promise – this is not the place to, for example, overstate your security program. Note that material changes to your privacy policy (such as a decision to share customer information with third parties) will require customer opt-in consent. Companies should also consider non-traditional and creative ways of providing notice to customers such as videos explaining privacy practices. Learn about [TRUSTe's Web Privacy Program](#).
- ➔ Do you use trustmarks?
  - Trustmarks and seals are a form of communication between consumers and businesses to help bridge the information gap about the security and trustworthiness of an online store. Define your goals and look for trustmarks that can help you achieve them.

## 9. Data Collection for the Future

The Internet is rapidly changing and allowing for new and expansive types of information collection. As users increasingly turn to mobile devices to surf the Internet opportunities to collect additional personal data points, such as a user's geographic location, increase. There's also a trend toward the broader integration of social networking technologies across the Internet, where social networks have opened up their reservoirs of user personal information and provided access to third parties such as advertisers and Web sites. As your company expands into the mobile and social networking fields, it's important that with each new data collection you stop to consider the unique privacy implications of the data collection and how these implications should shape your information processing practices and disclosures.

## 10. Conclusion

Navigating the sea of privacy rules, requirements, and best practices can be daunting but remember, you are not alone as privacy questions arise. TRUSTe Enterprise Services can help you fill privacy holes and help you create a more robust overall privacy architecture. Contact an Enterprise Solutions Executive to schedule an overview of your company's privacy practices today.

## 11. Privacy Assessment Checklist

Use the checklist below to gain a deeper understanding of your current privacy practices and assess your potential need to engage external privacy experts and resources to help you address shortcomings in your privacy programs and practices.

### Privacy Compliance

#### Who do you collect information from?

	Yes	No	I don't know
Do you collect information from children under 13?			
Do you collect information from people outside of the U.S.?			
Do you know what state(s) your customers reside in?			
Do you receive information about your customers from third parties?			

#### What data are you collecting?

Do you collect financial information?			
Do you collect health information?			
Do you access consumer reports?			

#### Do you have a plan in place to address a potential security breach?

Do you have somebody within the company who should be contacted immediately to avoid further data loss?			
Are there physical steps that should be taken to avoid further data loss?			
Do you have a plan for how the security incident will be investigated?			
Do you have notification requirements?			

If you answered "yes" or "I don't know" to three or more of these questions then you may have a significant privacy compliance burden. TRUSTe has helped thousands of business, small and large, address and comply with complex privacy frameworks and laws, from making sure a site's information practices comply with U.S. federal law protecting children online or EU law protecting the privacy of European citizens.

## Privacy Best Practices

### How are you collecting data?

	Yes	No	I don't know
Do you use cookies to collect data? Are you using session cookies, persistent cookies, Flash cookies?			
Do you use web beacons to collect data?			
Do you use embedded web links to collect data?			
Do you use other data collection tools such as tools that enable you to replay customer web sessions?			

### How are you storing the data you collect?

Do you store data in physically or electronically unsecured locations?			
Can employees access sensitive data not directly pertinent to their job function?			
Do you retain sensitive data longer than needed for its original use?			
Do you transmit unencrypted sensitive data?			
Do you delete or dispose of data without taking privacy precautions?			

### How do you use the data you collect?

Is the data you collect used for transactional purposes?			
Is the data you collect used for marketing purposes?			
Do you share information with third parties for the purposes of processing transactions?			
Are you using behavioral advertising to target specific customers?			

If you answered “yes” or “I don’t know” to three or more of these questions then you and your customers could benefit from external privacy resources to help achieve best privacy practices on your site. From data encryption to notifying customers of data collection and advertising practices, TRUSTe privacy experts are ready to help you create a comprehensive program to ensure you protect your customers’ privacy on your site.

## Privacy Best Practices

### Are you adequately communicating your privacy practices?

	Yes	No	I don't know
Do you have a privacy policy?			

If you answered “no” then you’re most likely in violation of California state law, which requires all commercial Web sites doing business with California citizens to have and prominently display a privacy policy on their Web site. Beyond compliance, having a privacy policy is sound business strategy: it’s a communication tool that helps reassure your customers that you respect their personal information and with 60 percent of site visitors reporting that they look at a Web site’s privacy policy it’s one tool you don’t want do be caught without.

Do you use Trustmarks?			
------------------------	--	--	--

If you answered “no” then you’re missing out on potential revenue and customers. Trustmarks from established and trusted third-parties like TRUSTe and Verisign signal to consumers that your site and its information practices have been vetted and approved - as a direct results consumers are more likely to do business on your site. Security seals like those offered by Verisign and McAfee can be used in tandem with a privacy seal from TRUSTe to achieve maximum returns on your trustmark investment.

## 12. TRUSTe Solutions

*TRUSTe's enterprise privacy services help thousands of leading Web sites increase conversion, meet global privacy standards and comply with privacy regulatory guidelines.*



### The TRUSTe Advantage:

#### ➔ Build Business

- TRUSTe online privacy seals have been shown to drive demonstrable business results on Web sites, resulting in increased conversions, greater sign-up rates, and higher average order values. Consider:
  - Wedding services provider ThePros.com increased purchases by 84% with the TRUSTe Privacy Seal. [Read more.](#)
  - Audible.com, and online provider of audio entertainment and education, saw a 22% increase in average order value with the TRUSTe Privacy Seal. [Read more.](#)

#### ➔ Build Global *Customer Confidence*

- Certify your privacy policies, resolve disputes, and communicate your privacy leadership in multiple languages using TRUSTe's international privacy services.

#### ➔ Mitigate your Risk with our Advanced Technology

- Leading-edge Web site privacy scanning to ensure compliance and assess impact of site changes to your privacy practices. Manage the privacy and brand reputation risks that come with using third-party services providers. Vet your contractors and third-party service providers with TRUSTe's Service Provider Evaluation services. [Learn more.](#)

#### ➔ An Independent Third-Party Dispute Resolution Service

- Provide your users with free online privacy dispute resolution and enable greater trust. TRUSTe resolves nearly 100% of consumer disputes every year.

#### ➔ Manage your Account through the TRUSTe Services Manager Portal

- Complimentary online account access to manage your privacy programs, track disputes and review scan results.

#### ➔ Demonstrate your Commitment 24/7 through your Validation Page

- Over twenty million consumers click on the TRUSTe seal every year to confirm site validation, while over a million consumers have endorsed the privacy practices of TRUSTe clients.

Contact an [Enterprise Solutions Executive](#) to schedule an overview of your privacy practices today or call (415) 520-3490.