



Privacy Primer: Protecting the Consumer in the Age of Behavioral Targeting

About Openwave

Openwave Systems Inc. (Nasdaq: OPWV) is one of the world's leading innovators of software applications and infrastructure designed to enable revenue-generating, personalized services, including mobile analytics, content adaptation, mobile and broadband advertising, and a suite of unified messaging solutions.

As the communications industry intersects with the Internet, Openwave software enables service providers to converge services, in an effort to increase the value of their networks by accelerating time to market and reducing the cost and complexity associated with new service deployment. Openwave's unique product portfolio provides a complete range of mobile internet service management, messaging, and location based solutions. Openwave is a global company with a blue chip customer base spanning North America, Latin America, Australia and New Zealand, Asia, Africa, Europe, and the Middle East. Openwave is headquartered in Redwood City, California.

For more information please visit www.openwave.com.

Openwave and the Openwave logo are registered trademarks of Openwave Systems Inc. in various jurisdictions. All other trademarks are the properties of their respective owners.

Copyright © 2009 Openwave Systems Inc. All rights reserved. April 2009.

Privacy Primer: Protecting the Consumer in the Age of Behavioral Targeting

Table of Contents

Introduction	4
Spotlight on Privacy.....	4
Technology.....	4
Globalization.....	4
Regulatory Groups.....	4
Public Awareness and Expectations	5
Rethinking Privacy	5
Mobile Privacy.....	6
Invasion	7
Collection.....	7
Processing	7
Dissemination	8
The Principals of Privacy Management.....	8
Disclosure	8
Keep the User in Control	8
Organizational Commitment to Privacy.....	9
Understanding the Laws	9
Executing Privacy Management.....	10
Conclusion	11
Appendix: Laws that Impact Privacy.....	12
United States	12
Canada	12
Europe	12
Asia Pacific and Japan.....	12

Privacy Primer: Protecting the Consumer in the Age of Behavioral Targeting

Introduction

Soliciting and understanding customer feedback is essential to running a successful business. On the internet, customer feedback isn't requested so much as it's collected, like a digital trail of breadcrumbs. Mobile technology only sharpens the focus on user behavior by bringing location and contextual information into play. As a result, mobile operators are getting closer to that “360-degree-view” of their subscribers: the foundation for improved customer service, better products and a more personalized experience.

The ease with which consumer behavior can be tracked online raises obvious concerns about an individual's privacy. At the top of the list is the protection of personally identifiable information (PII) like a social security number, bank account number or home address. But even non-PII (one's gender, age or city of residence) in the wrong hands could lead to identity theft.

The purpose of this primer is to look at the privacy issues facing mobile operators and others in the value chain. The mobile medium is the most personal because of its one-to-one relationship with the user – we don't share our phones. Mobile devices have the ability to register a user's location, and for a growing number of people, they serve as a digital wallet, holding photos, music and other personal information. As more users spend more time connected to online communities through their mobile device, striking a balance between user benefits and personal privacy is essential for the mobile operator, especially as behavioral targeting and mobile advertising gain traction in the marketplace.

Spotlight on Privacy

New technology, globalization, regulatory groups and an overall increase in public awareness and expectations have raised the issue of privacy to the forefront of the mobile industry.

Technology

The proliferation of high-speed wireless networks supporting smartphones and a burgeoning mobile application business have improved the user experience. As consumers do more with their phones, they leave behind a digital trail that can be tracked and analyzed by various players in the value chain. Also, the availability of cheap storage allows companies to easily store and access terabytes of consumer behavior data.

Globalization

The diminishing digital boundaries between nations have created new global communities that can communicate seamlessly over the Internet. In the same way, multinational companies are optimizing how they do business, sharing customer data across the globe.

Regulatory Groups

To protect consumer and business privacy, state and federal governments have enacted regulations and created separate bodies to deal with the various lobbying groups. The European Union, Canada and the United States have several statutes enacted to cover privacy (see appendix on page 12).

Public Awareness and Expectations

Due in part to the numerous regulatory groups formed and privacy lawsuits filed over the last decade, consumers are more aware that their personal data can be viewed and shared. According to a recent survey by Burst Media, 60% of users are aware that personal information is collected as a result of online activities.¹

According to another survey conducted by independent privacy consultant group TRUSTe.com, online privacy remains overwhelmingly important to consumers, but consumer discomfort with behavioral tracking had declined more than 6% in the last year.²

Respondents Saying it is Likely Web Sites are Collecting PII and Non-PII Information

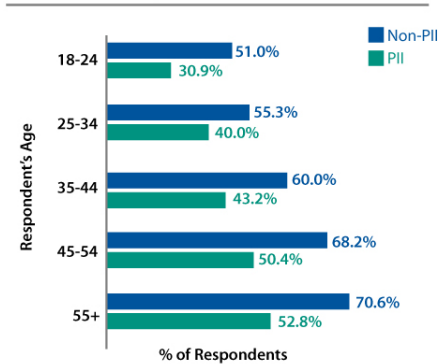


Chart 1: Respondents Who Believe Sites Collect PII and Non-PII Information
Source: Burst Media, December 2008, n=4,011
Margin of Error: +/- 1.5%

BurstMedia

Agree/Disagree with Websites Collecting Non-PII to Target More Relevant Ads

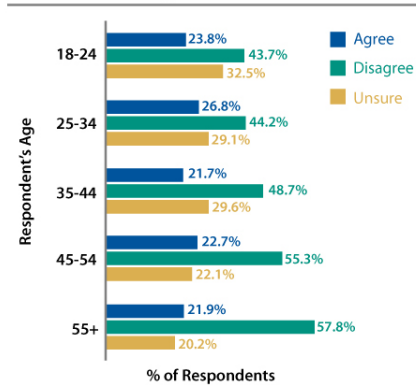


Chart 2: Respondents Who Agree or Disagree with Websites Collecting Non-PII to Target More Relevant Ads
Source: Burst Media, December 2008, n=4,011
Margin of Error: +/- 1.5%

BurstMedia

Rethinking Privacy

Privacy agreements can be viewed as an exchange of personal information (PII or otherwise) for some clear and significant benefit. For example, a user submits his bank account number for the convenience of online banking. In some cases, companies use personal information to offer targeted ads which subsidize their communications products or premium content. Companies can also track where a user goes online to optimize their network or improve their products and services.

When we think about privacy in the context of the internet (mobile or broadband) we need to pay attention to what data is passing through the system. Figure 1 shows the kinds of data that could be left as part of a user's digital trail. These elements have been organized into four groups depending on their identification capability (PII vs. non-PII) and how long the information stays in the digital universe. The amount of data left on websites, search engines and blogs is hard to quantify but as storage becomes cheaper, pressure to clear old data diminishes. With more data being stored, enough non-personally identifiable information can be collected that, when taken as a whole, make a user personally identifiable.

¹ Burst Media Survey: Online privacy still a consumer concern: http://www.burstmedia.com/assets/newsletter/items/2009_02_01.pdf

² TRUSTe.com: 2009 Study: Consumer attitudes about behavioral targeting

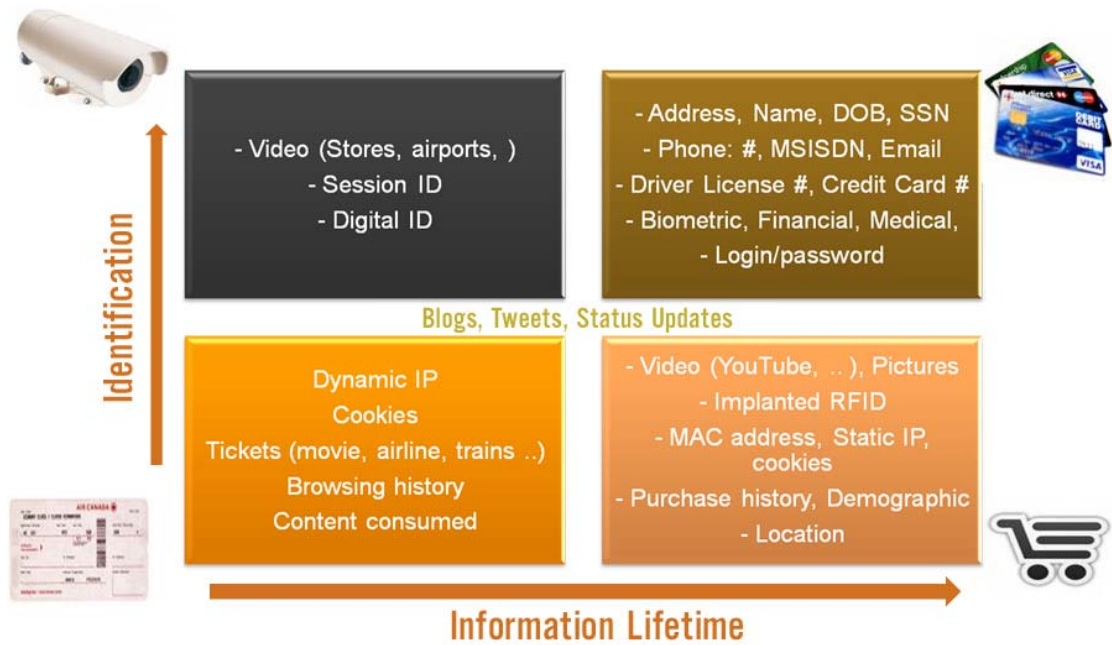


Figure 1: Various data elements

Mobile Privacy

Nowhere is privacy a bigger issue than in the mobile space. Mobile phones are personal, always-on, location-aware devices that users carry with them throughout the day. And unlike broadband operators, mobile operators wield far more control over their networks. With such power, mobile operators are often accused (rightly or wrongly) of being the biggest threat to privacy. This has created challenges for companies whose business models depend on processing and using subscriber data. Figure 2 illustrates some of the issues in the mobile value chain³.

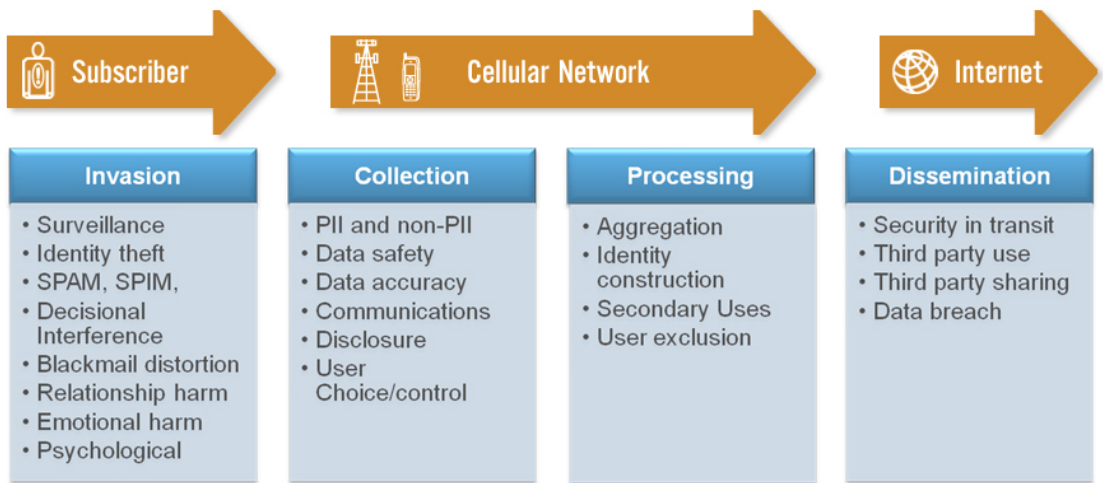


Figure 2: Privacy issues in mobile chain

³ Daniel Solove: Understanding Privacy

Invasion

Invasion is the misuse of personal data which can exist in many forms, such as:

- **Surveillance:** when a mobile device is used to track different kinds of subscriber activities e.g.: voice, location, internet activity, content (pictures, music) internet downloads.
- **Identity theft:** when personally identifiable information such as a credit card number or driver license number is intercepted by a rogue entity and misused.
- **SPAM, SPIM or SMS SPAM:** the use of phone numbers or email addresses to send unsolicited email, SMS or instant messages. Although SMS spam is illegal in most jurisdictions, email spam may not be.
- **Decisional Interference** is when one party uses persuasion or threats to interfere with another party's decisions about his livelihood or that of his family.

Collection

The central issue at the data collection phase is disclosure. Users must be told in very crisp and clear terms what information elements are stored and used. Such disclosure should answer the following questions:

1. Type of data:

- a. What data is being collected? Is this data strictly related to the product or service's benefit?
- b. How often is data collected? How long is data stored?
- c. Is data kept safe or encrypted? Who has access to data? Are they trained? What are the processes in place to safeguard data?

2. Use of data:

- a. How does the user benefit by agreeing to share personal data?
- b. How exactly is the data being used?
- c. If the original use changes, how do you notify users?

3. Sharing of data:

- a. With whom is data shared?
- b. Are those third parties trustworthy?
- c. Do they have processes in place to keep data safe?

4. Communication:

- a. Is there a mechanism in place to address the questions above and communicate them with the user?
- b. Is it presented simply and in clear terms?
- c. Are users presented with a clear choice to opt-in, opt-out or otherwise control what data can be shared?

Processing

The processing phase deals with taking the stored data and combining it with other pieces of information. The issues that could arise in this phase are:

1. **Aggregation:** The combination of various information elements about a person. Combining bits of personal information exposes more of an individual's identity.
2. **Identity construction:** Non-PII can be combined with other non-PII to construct a clearer picture of the person. Such instances may occur when an IP address is associated with a billing record to identify a person. Note: It is said that most people can be personally identified with only three pieces of non-PII information: zip code, date of birth and gender.
3. **Secondary use:** Using data for something other than what was promised to the user.

4. **User exclusion:** Generating information on behalf of a user that he may not know about. User exclusion is a common in identity theft which can affect the victims purchasing history, credit rating and in some cases reputation.

Dissemination

Issues around dissemination arise at the point where processed information is ready to be shared with third parties, for example:

1. **Data security in transmission:** Sensitive PII becomes vulnerable to theft if it is exchanged in clear-text.
2. **Third-party use:** User must be aware that data is being shared with a third party.
3. **Third-party sharing:** User must know that a third party is sharing data with other third parties.
4. **Data breach:** If a third party or primary party loses user data, users must be informed.

The Principals of Privacy Management

The goal of privacy management should be to build relationships, increase trust and provide users with a safe environment to participate. Anything less jeopardizes business goals and user security. The following are the pillars of a sound privacy management policy.

Disclosure

The most important part of a privacy policy is disclosure: being upfront and honest with users about the collection and use of their personal data. Privacy policies should be stated in clear and concise language (not legalese) and be easily accessible.

Full disclosure will identify what kind of data is being captured, how it will be used, how long it is stored and how it is or will be shared with others. If the technologies used to collect or track user behavior are new, it is wise to educate users about such technologies in simple language. This knowledge will help users understand the benefits and alleviate possible fears.

If there is a material change to an existing privacy policy, users must be informed of such changes and in some cases asked to accept these new changes as part of the usage agreement.

NOTE: Special disclosure considerations are required to be complied with for certain age groups (e.g. under 13 years old or 13-18 years old).

Keep the User in Control

The second principal of privacy management involves giving the user clear control over how his information is used. A link to the privacy page or control panel should be obvious to users. A privacy control panel should include the following:

1. Opt-in or opt-out of certain applications or programs*
2. Preferred delivery methods (e.g. email, SMS or IM) and frequency, if applicable
3. Ability to modify or delete one's own data
4. Option to share data with third parties
5. Mechanism to report abuse
6. Ability to change any of these settings at any time

* Opt-in or opt-out can be bound by legal requirements (i.e. parental consent is needed for underage children).

New applications like location-based services that use highly private information should provide frequent reminders about the privacy settings. Google Latitude and Yahoo! Fire Eagle are two examples of such a practice.

Organizational Commitment to Privacy

Privacy management is more than just implementing a transparent privacy policy. It is an ongoing effort to honor the promises made in the policy. Organizational commitment to privacy includes education and proactive industry engagement.

Educating your customers, your employees and government bodies about privacy pitfalls and best practices is an important step towards a full solution. As stated above, education should be part of a good privacy policy, but clear links to outside resources should also be available to consumers.

Industry groups need to work closely with consumer advocates, government and other non-profit groups to discuss and propose privacy solutions. Co-developing self-regulatory principles can help in obtaining buy-in from government bodies.

Proactive engagement with industry groups like the Center of Democracy and Technology (CDT), TRUSTe, Mobile Marketing Association, Privacy International, International Association of Privacy Professionals is the best way to participate in the privacy debate and learn about industry-accepted best practices (figure 3). The more your company is monitoring and contributing to the debates the more prepared it will be.

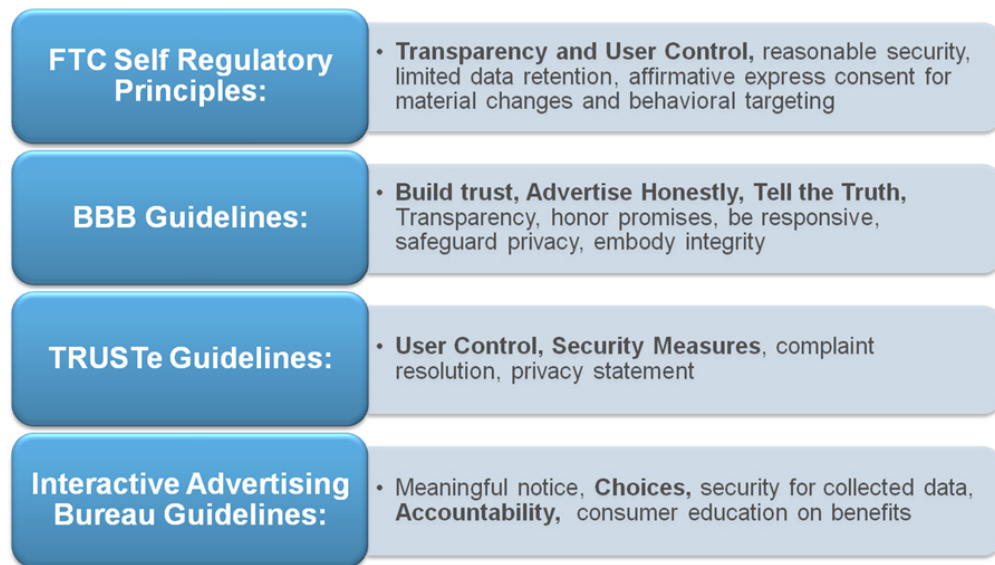


Figure 3: Sample best practices from leading industry groups

Understanding the Laws

Over the years, new technologies like the telephoto lens, microphone, video recording, webcam, etc., often required old laws to be revisited, changed or scrapped altogether. Different countries have their own set of privacy laws (see appendix on page 12). When developing privacy policies it is important to take into account the laws of each particular region in which your company operates. Below is a checklist of items to look for when reviewing local laws.

1. Check for scope:
 - a. What is the definition of personal data, how is personal identification information (PII) defined and treated?

- b. How is data processing defined? How does this definition impact the value proposition of a particular offer or service?
 - c. What jurisdictions apply? Can sensitive PII data be transferred outside this jurisdiction? Who can data be shared with and what are the expected standards of data security?
 - d. What are the disclosure standards of the region?
2. Check for consent rules:
 - a. What type of information requires opt-out or opt-in?
 - b. How is consent captured? Is electronic consent acceptable?
 - c. Can minors give consent? Is parental consent required? How is are minors' personal data handled (i.e. can their profiles be searched)?
 3. Check the International Data Transfer rules for the countries in which you want to do business.
 4. Check for Binding Corporate Rules (BCR), global privacy policies that govern the transfer of sensitive corporate data (customer databases and HR information) outside Europe.

Executing Privacy Management

Rolling out a complete privacy framework is a four-phase process (figure 4). In the analysis phase, companies weigh the customer benefits against the information required to deliver those benefits. Research, focus groups and/or outside studies will show how different user groups (age, geography, gender, etc.) will react to the proposed method of data collection and usage. These results can be essential to product design. It is wise to engage with legal privacy experts early to avoid surprises later. Risk analysis prepares companies should user data be compromised.

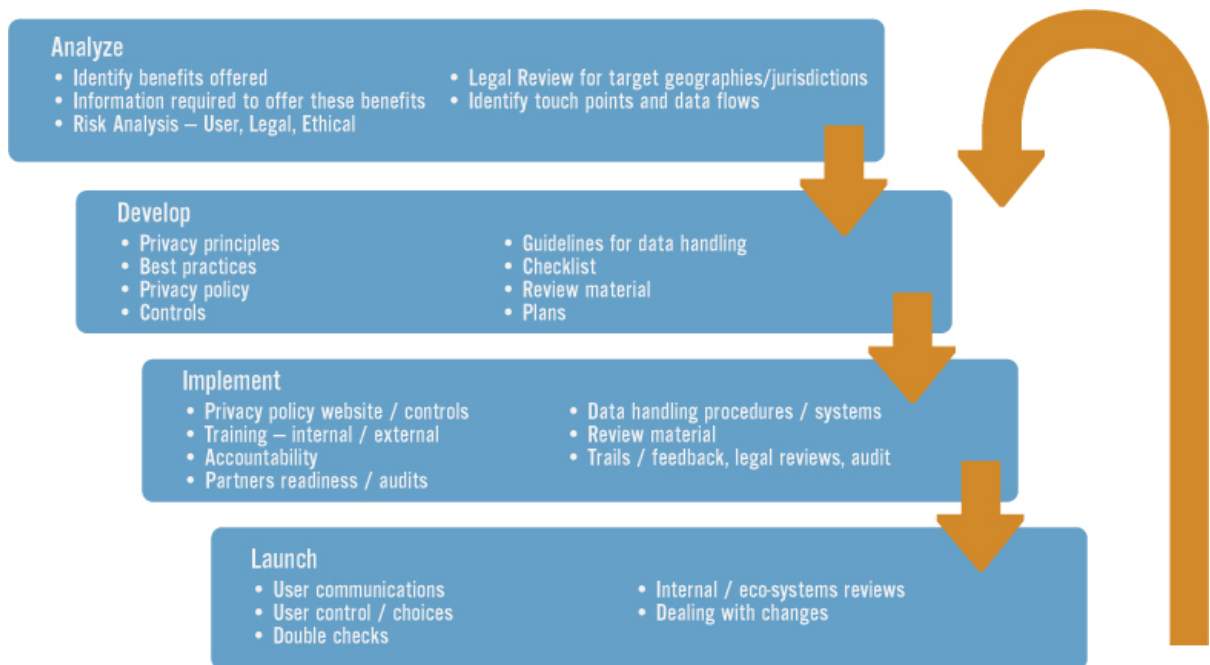


Figure 4: Sample process for effective privacy implementation

The next phase is the development of the principles, best practices and privacy policy itself. Document what data is necessary and what age-appropriate privacy controls are presented to the user. Engage appropriate groups in other parts of the organization and the broader industry ecosystem that are impacted by the privacy policy.

The implementation phase is where the product and processes around privacy are built. You should begin by: educating internal and external stakeholders about privacy and ways to deal with it; developing and auditing data breach and consumer communications plans; and conducting reviews through stakeholders and competent third parties. One of the key elements of this phase is to establish accountability. To that end, some organizations appoint a Chief Privacy Officer.

As new products and services hit the market, there will be temptation to collect and use more consumer data. Practice *data minimalism* and resist such temptations, weighing them carefully against the benefit they offer to users. Other techniques include:

1. **Anonymization** – remove personally identifiable information at an early stage of collection
2. **Deletion** – delete data after use expires.
3. **Isolation** – isolate data among various processing modules.

Before you are ready to launch the product or service, do a limited trial. A trial can provide an opportunity to obtain early reaction from a sample audience. Figure 4 shows additional best practices in use today.

Conclusion

In many ways, the mobile industry can follow the broadband industry's lead with respect to privacy management, but more work must be done. Of all the mass media, mobile has the power to reach the farthest and get the closest to consumers.

Armed with a good mobile analytics tool, the mobile operator, more than any other member of the value chain, can do the most good or the most harm. Online behavior (from click stream logs), demographics data (from the billing relationship) and location data (from GPS or cell towers), if aggregated and analyzed correctly, presents the most complete consumer view to date. With this 360-degree-view of the consumer comes responsibility.

As mobile devices continue to evolve past phones with voice capabilities only to become the central device that controls our digital lives, mobile operators must lead the way in establishing the right privacy framework that fosters trust every step of the way. Privacy policies must be easy to find, easy to read and easy to understand. They must map to specific user benefits and, most importantly, they must place the control with the user. Then and only then will the mobile experience, including behavioral targeting, reach its full potential.

Appendix: Laws that Impact Privacy

United States

Federal Laws:

- Context set in 4th Amendment
- FTC Act 1914, Amended in 1938, 1994
- Telecommunications Act of 1934
- Federal Wiretap Act of 1968
- Fair Credit Reporting Act of 1970
- Privacy Act of 1974
- Cable Communications Policy Act of 1984
- Computer Fraud and Privacy Act of 1986
- Electronics and Communications Privacy Act (ECPA)1986
 - Includes Stored Communications Act
- Video Privacy Protection Act of 1988
- Health Insurance Portability & Accountability Privacy Act of 1996
- Gramm-Leach-Bliley Act (Financial Privacy Rule) 1999
- Children Online Privacy and Protection Act 2000

State Laws:

- CA: Invasion of Privacy Act
- CT: Confidentiality of SSN (Public Act 08-167)
- MA: Standards for the Protection of Personal Information Act
- NV: Restrictions on transfer of personal information through Electronic means (mandates encryption)
- NY: Use of personal information without consumer consent

Canada

- Privacy Act of Canada (R.S. 1985)
- Personal Information Protection and Electronic Documentation Act (PIPEDA)

Europe

- EU 95/94/EC directive on processing of personal data and free movement of such data
- EU Article 29 Data Protection Working Party related to BCR (Binding Corporate Rules) – WP 155
- UK: Data protection Act of 1988
- French Data Protection Authority (CNIL)

Asia Pacific and Japan

- Australia: Privacy Act of 1988
- Japan: PIPL (Personal Information Protection Law)

Authors

Openwave Systems Inc.

Feedback

To receive more information about Openwave's mobile internet services including Mobile Analytics, email: marketing_ww@openwave.com



Openwave Systems Inc.

2100 Seaport Boulevard

Redwood City, California 94063 U.S.A.

Corporate +1 650 480 8000

Europe +44 2890 416 200

Asia +81 3 5909 6100

<http://www.openwave.com>