ORACLE9I PRIVACY PROTECTIONS

Kristy Browder Edwards, Oracle Corporation

EXECUTIVE OVERVIEW

Every organization that collects any personal information from its customers is responsible for protecting the privacy of that data. Privacy protection is becoming a decision making criteria for the software buyer and a product differentiator for the vendors from whom they purchase IT products. Privacy is not just a compliance requirement, it is good business.

INTRODUCTION

The ways in which you use, manage and distribute personal information is part of your customer's determination of how much they will trust you. Organizations entrusted with an individual's personally identifiable information cannot afford to overlook the importance of keeping private the data they collect. Further complicating matters, your partners' compliance with regulations impact your business.

Reliable privacy protection is something you cannot afford to dismiss. With the right combination of secure software, sound implementations, and careful privacy policies, you are empowered to protect the privacy of your users', employees' and customers' personal data.

THE IMPORTANCE OF PRIVACY

Vendors like Oracle must examine privacy protections and ship products that can be part of customers' implementations that keep the world's data safe. Customers of Oracle (those who purchase and run Oracle software) must take steps to keep their customers' personally identifiable information confidential. In turn, business partners should keep check on one another's privacy policies and practices.

PRIVACY AND SECURITY

To begin the discussion, let's define the relevant terminology. In the vernacular of privacy, the individual or customer whose personal information is in question is called the ***data subject***. The service provider or IT organization is referred to as the ***data collector***. The concept of a collector is further differentiated into ***data controller***—a party that exerts some dominion or control over the information—and ***data processor*** who merely executes certain technical measures and functions to the data pursuant to the direction of a controller. Personal or confidential information collected about a person that can be tracked back to him/her or is associated with an individual's identity is called p***ersonally identifiable information*** (PII), and PII is the precious data that is at stake. All organizations that collect personal data should develop a ***privacy policy***, in which they disclose what information is collected, why and how it is used, and who it is shared with. Privacy policies can only be developed after careful inquiry into what your privacy practices actually are.

Depending on the nature of the privacy policy, it may give consumers the choice to "***opt-in***" or "***opt-out.***" That is, consumers actively communicate whether they will participate in data collection via an opt-in mechanism, whereas opt-out procedures mean that users must take action to revoke their participation. Most importantly, ***privacy*** and ***security*** relate closely to one another, and while they are not synonymous, they can be implemented in complementary and reinforcing ways.

Privacy involves the subject's rights, choices and control over the use of personally identifiable information. The subject must be informed of the usage of his or her information, be allowed to request access to the data, request correction of any misinformation, and have the assurance that the data collector adequately protects her information. Such protection includes the use of appropriate security precautions.

Security is the protection of data from unauthorized access. Its main tenets are confidentiality, integrity and availability (CIA) of data. Security entails establishing the identity of users, preventing unauthorized access to systems, maintaining data availability for—and only for—its intended recipients, preventing data corruption and insuring its validity, and maintaining accountability of users. Security, however, is broader in scope and has uses that go beyond the protection of PII. Security is necessary but, alone, not sufficient for privacy.

To summarize their definitions:

- Privacy: the data subject chooses among preferences about the use, collection and sharing of personal data, and the data collector uses information for the purposes specified and protects the subject's information.
- Security: the protection of data from unauthorized access, with the foundation of confidentiality, integrity and availability of data.

What is the relationship between privacy and security? Information security is a fundamental component of privacy, while privacy also fundamentally includes policy, usage, access to one's own records. They both have distinct yet overlapping footprints. Security can exist without privacy, but privacy cannot exist without security.

Consider a financial institution that implements top-notch security solutions with strong user authentication, 128-bit encryption, hardened operating systems, and proper personnel and physical security in place. Regardless of tight security controls, the organization denies its customers access to their own information to monitor its accuracy, and it allows a third party to access PII without notification of the subject. This implementer may have a reasonable security implementation but lacks sufficient privacy protection and compliance.

On the other hand, true privacy cannot exist without adequately employing security. Consider an Internet Service Provider (ISP) who diligently considers personal privacy outcomes of every one of its policy decisions. They neither share nor sell any user's personal data. They strictly prohibit unauthorized users from accessing customer records. This ISP always allow the end users to view and correct information about themselves. Yet with all of these safeguards, the ISP has not achieved adequate privacy unless they have purchased and deployed the security mechanisms necessary to protect their users' personal data assets.

This paper explores some of those security mechanisms and their application to privacy. First, for context, the report looks at regulations, initiatives and laws that protect our privacy. For there is no way to safeguard users' PII without understanding local and/or international mandates under which you and your partners operate. Second, it details how the IT industry addresses privacy through proposed standards, third party services, and finally, software solutions. These solutions empower purchasers and implementers to handle PII with the privacy safeguards it deserves.

REGULATIONS

Privacy regulations are not new. The first privacy legislation and regulation were enacted in countries around the world long before the Digital Age and the explosion of the Internet. The right to privacy is a well-established constitutional edict in countries from Asia to North America, Europe to South America. Law relating to privacy can be tracked through the ages, with great emergence of new privacy-specific laws around the world beginning in the 1960's.

U.S. REGULATIONS

FEDERAL

Significant Federal privacy regulations began appearing in the US in the 1970's, most notably the Privacy Act of 1974. This important law protects records maintained on individuals in the U.S. The Family Educational Rights and Privacy Act (FERPA), safeguarding the privacy of student education records, surfaced in the same year. The Fair Credit Reporting Act (FCRA) was enacted in 1970, and, in 1996, was amended extensively. The FCRA deals with privacy protection related to information on an individual's creditworthiness and defines related responsibilities and liabilities of businesses. All three of these laws are applicable to companies and organizations today, whether they are government, brick-and-mortar or e-commerce players.

With the advent of the Digital Age, computer privacy acts began emerging. The Computer Security Act of 1987 by NIST (the National Institute of Standards and Technology) regulates "sensitive but unclassified data" and was among the first computer security or privacy initiatives with significant impact in the U.S. The Children's Online Privacy Protection Act (COPPA) of 1998 mandates verifiable parental consent before a web site collects any child's personal data. Also in 1998, the FTC (Federal Trade Commission) submitted a report to Congress focused on protecting consumer privacy on the web.[i] The FTC report is often called upon in privacy matters for its emphasis on the basic privacy principles:

- Notice—data collectors must inform consumers of their information practices;
- Choice—consumers have the right to choose how personal information is used when it is used for a purpose other than the original purpose for collection;
- Access—consumers can view the accuracy of data collected about them, and they have control in making changes to correct inaccuracies;
- Security—data collectors shall take reasonable actions to ensure the accuracy and security of the data.

These four principals surface regularly in the context of privacy. They figure into the most significant regulations today, including HIPAA and Graham-Leach-Bliley.

In the past year, digital privacy acts have appeared with speed. As of the writing of this paper, a number of bills and regulations are sweeping political institutions around the world. In the U.S. alone, such bills are moving through local, state and federal legislative processes. For example, the Electronic Privacy Protection Act, currently in the House of Representatives, prohibits use and distribution of "information collection devices without proper labeling or notice and consent." [ii] The Online Privacy Protection Act of 2001, also in the House, focuses on privacy protections of personal information. The California financial privacy bill is just one of the bills in process at the state level within the U.S. Similarly, local municipalities are creating laws to protect their residents.

STATE REGULATIONS

Apart from Federal bills, there has been an explosion of laws related to privacy within the states. The vast majority of the privacy bills to date have related to spam or identity theft, but more specialized bills related to financial and health information have been passed as well.

These privacy-related bills have implications on how information must be secured, how and to whom it can be transferred, and under what conditions and with what required permissions. From a compliance perspective, these laws increase the complexity of solutions by multiplying the factors and jurisdictions involved, as well as creating issues of associating individuals with locations. In a world where so many goods can be delivered electronically, identifying an individual's location for compliance purposes can be a challenge. Nonetheless, states that participate in privacy laws are taking strides to protect their residents like those privacy mandates at the Federal level.

INTERNATIONAL REGULATIONS

Beyond the borders of the United States, there has been even greater regulatory activity regarding privacy. In countries around the world, the right to privacy is guaranteed as a fundamental human right. More recently, many European countries enacted modern privacy legislation beginning in the 1970's. The United Nations has written legal documents regarding the protection of personal information. Singapore, Hong Kong, middle eastern and other Asian countries and commonwealths legislate privacy protections for electronic and non-electronic information. Likewise, Australia, South American and North American countries protect citizen's privacy through legislation.

In 1980 the Organization for Economic Cooperation and Development (OECD) set forth a set of Guidelines for the Protection of data and trans-borderr data flows that is regarded by many as the clearest statement of an international privacy standard. In 1981, the Council of Europe produced a treaty instituting protections for personal data. The European Commission's Directive on Data Protection, a far-reaching privacy regulation, has been in place since 1998.[iii] This privacy initiative provides for protection of European Union residents' personal data both within Europe and beyond. In order to assure "adequate" PII protection of EU residents, the EU has been going through adequacy evaluations. To date the laws in Hungary, Canada and Switzerland have been found to be "adequate." The US laws were not found to be adequate, but companies, like Oracle Corporation, that self-certify to a set of principles called the Safe Harbor have been found adequate as well.

THREE SIGNIFICANT REGULATIONS

THE SAFE HARBOR

The Safe Harbor extends privacy protections for residents of the European Union (EU). The Safe Harbor sets out the conditions under which PII may be transferred from the EU to the US absent other ways of complying with the EU Directive. One key element of Safe Harbor is the "onward transfer" of information. [iv] Onward transfer is noteworthy because it regulates not only the holder of an EU citizen's personal data, but also the holder's release of that data to another entity. The focus of much international legislation addresses the need to deal with transfers and onward transfers of information across multiple jurisdictions, such as the numerous jurisdictions involved in servicing client accounts for a global enterprise that provides 24x7 service.

The Safe Harbor's basic principles are notice, choice, transfers to third parties, access by the individual (subject), and security rendered by organization collecting personal data. As well, its founding principals regulate data integrity (meaning the relevance of the information) and enforcement (or providing a means of recourse).[v] Interestingly, Safe Harbor regulations apply to 'one-hop' sharing only. That is, participation in the Safe Harbor agreement between EU and US institutions does not necessarily allow the US entity, in turn, to share information with a partner in South America absent certain contractual provisions for the consent of the data subject. These restriction go to great lengths to protect the privacy of individuals in Europe.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is U.S. legislation with a compliance deadline of April 2003. Its reach extends far beyond privacy; it is fundamentally designed to reduce the complexity of information transfer between healthcare organizations and partners. HIPAA has two separate rules, one on security (that is in draft) and one on privacy (that has passed). The privacy rule was added to HIPAA in December 2000 regarding its standards for privacy of individually identifiable health information. The addition gives a patient the right to access and control the usage of his health records and puts the burden of PII protection on healthcare providers.

The HIPAA legislation is complex and far-reaching. It impacts many types of businesses and organizations, including those you might expect, such as healthcare providers, healthcare payers (e.g., insurance companies), and those who do business with health-related organizations. What's more, it applies, either directly or through "business associate"

requirements, to non-healthcare providers such as technology partners including Internet Service Providers (ISP) and Application Service Providers (ASP), financial institutions, and virtually any other organization that works with healthcare establishments.

What makes HIPAA unique in a wave of international regulations in diverse industries are its security mandates. HIPAA proposes security requirements for the following:

- *Policies and administrative processes* to protect patients' personal data by means of documented Information Security measures;
- *Physical safeguards* protecting buildings and computer systems from threats ranging from fire to intrusion;
- *Technical data security processes* to protect, control and monitor access to personal data;
- *Technical security measures* to protect unauthorized access to data on a network.

These security measures render much more descriptive digital security requirements than other privacy regulations. Still, HIPAA does not mandate specific technologies or standards a data collector (or partner) must implement. It does not establish the exact policies and processes you must observe. The responsibility to select, purchase, implement, configure, and maintain the proper equipment and products falls onto the organization collecting or using patients' personal data.

GRAMM-LEACH-BLILEY

In addition to the HIPAA regulations that some financial institutions may be obligated to comply with, the financial industry has its own laws to adhere to. The Gramm-Leach-Bliley Act (GLBA) of 1999 also contains privacy and security provisions, and GLBA has been in effect since late 2000. The law permits banks, insurance and brokerage companies to affiliate under certain conditions, and it carries a number of privacy and disclosure provisions.[vi] Consumers are probably aware of this privacy law because their banks notified them (by mail) with a letter or booklet detailing their bank's privacy and information sharing policies.

The law stipulates that financial institutions shall disclose their privacy policies with consumers and customers upon establishing the customer relationship, then annually thereafter. The data collector is to describe the types of data collected, whom (organizations and personnel) they share data with, and how they share information about current and former customers. Similar to the Safe Harbor, third parties who receive personal information are bound by the same disclosure limitations as the data collector. Finally, before the institution shares information with nonaffiliated third parties, it must allow the consumer to "opt-out" of sharing her information. Like other regional and industry-specific regulations, it does not stipulate the use of particular products nor implementation of IT security standards.

SUMMARY OF REGULATIONS

These electronic privacy protections have the common themes of notice, choice and security. Common also is the absence of mandates on the use of specific products, security measures, or industry standards.

PRIVACY CERTIFICATIONS, STANDARDS AND PRODUCTS

Efforts are under way to establish standards for privacy, and, in parallel, independent organizations have formed to provide "privacy certifications" for web sites.

PRIVACY CERTIFICATIONS

Independent companies have emerged for the purpose of generating privacy certifications, primarily for web site producers who wish to establish an independent measure of their privacy practices. These third-party companies check a site's privacy statement against pre-determined acceptable standards and verify that the statements are properly enforced. If the site meets the privacy certification requirements, it may display the certification company's

privacy seal on its web site. Consumers may use the privacy seal to determine whether or not to do business with the company. TRUSTe and BBB Online are the most recognized seals.

Oracle Corporation's privacy policies have been reviewed by TRUSTe, and Oracle has obtained TRUSTe's Safe Harbor seal. Oracle Corp. is listed by the Department of Commerce as one of the companies certified with Safe Harbor.

STANDARDS

PLATFORM FOR PRIVACY PREFERENCES - P3P

The most widely known draft standard is the World Wide Web Consortium (W3C)-produced Platform for Privacy Preferences (P3P) draft standard, which enables consumers to select from a number of conditions under which they will divulge personal data to web sites. P3P user agents can be integrated into browsers, browser plug-ins, or proxy servers. The standard makes it possible for the user to determine a site's privacy policies as a means to decide whether it will allow information to be collected. User agents compare the user's privacy preferences—for example, permission to collect her email address but not her full name and mailing address—with the site's policy.

P3P provides an Extensible Markup Language (XML) schema that defines the purpose, recipients, types, and categories of personal information collected. P3P has mandatory and optional components. The optional components allow a user to "opt-in" or "opt-out" of particular types of data collection. Opt-in means that the user takes an action to participate, whereas opt-out means that users must take action to revoke their participation. P3P is a platform designed to protect individual privacy while enabling the exchange of personal information within user-specified limits.

CPEXCHANGE

The Customer Profile Exchange, or CPExchange, specification defines for an enterprise a profile on a customer or business partner. CPExchange associates privacy controls with subsets of profile information. It allows for the query, delivery and update of profile information, which uses XML to represent the data. This specification represents another privacy model whose proponents are attempting to gain traction across industries.

PRIVACY ENHANCING TECHNOLOGIES AND ANONYMIZERS

Privacy Enhancing Technologies or PETs are technology products whose main purpose is privacy. The Oracle database is not categorized as a PET because its main function is not privacy; it is a tool that facilitates privacy-enabled implementations.

Anonymizers are products which strip out PII or provide fake information in place of actual personal information associated with an individual. These products should be used with some level of caution, as anonymizers themselves have the ability to aggregate PII. Thus, the user shifts his trust from various web sites collecting segments of his personal data to one anonymizer whose job is to protect significantly more, aggregated PII.

SUMMARY

Thus far, privacy standards have not gained mass appeal, and privacy certifications are gaining momentum. One of the difficulties with using industry standards to establish privacy protections in your business is that privacy relies as much on administrative policies and procedures as it does on following standards and using secure products. It is difficult to standardize business models. Your policies will vary, but Oracle Corporation, and all of the vendors you choose, should be committed to providing you the tools for establishing privacy protections.

ORACLE'S ROLE IN PRIVACY

Can a vendor sell a privacy-enabled product? What role does a software product like the Oracle9*i* Database play in privacy? How does a privacy-conscious data collector make IT purchase decisions? As established earlier, security plays a role in privacy, and privacy is more than the sum of product features. Privacy protection requires an amalgamation of secure products, sound implementations, and suitable policies and procedures followed by the data collector.

No product can single-handedly safeguard personal data, and IT buyers do not select a software product without considering the hardware, operating system, other applications and infrastructure products also deployed. Likewise, IT buyers (software implementers) consider the privacy-enabling solutions offered in the products they purchase. Because it is the software implementer's duty to protect their customers' privacy, Oracle Corporation develops features and solutions to support its customers' privacy obligations.

Oracle Corporation is taking a leadership role in privacy. The lead results from the convergence of effective product strategy, the completion of internationally-recognized independent security evaluations, and product solutions unmatched by any vendor. Customers of Oracle are able to leverage its security solutions in their implementations in order to protect the personally identifiable information of their customers, users, and partners' users.

ORACLE9I DATABASE STRATEGY FOR PRIVACY

Privacy cannot exist without security. It is impossible for you, the implementer, to comply with your industry's regulations and your own corporate privacy policy if you make the wrong choices about the products you deploy. A secure foundation is necessary, though not sufficient by itself, for privacy. If you deploy software that is proven to be secure, you are on your way to running a successful, privacy-aware business.

Secure solutions lend themselves to privacy-centric implementations. How do Oracle's customers know they can rely on the Oracle9*i* Database for privacy?:

1. Assurance. A provably-secure product, backed by multiple independent security evaluations, lends itself to a privacy-centric deployment.
2. Data-Centric Security. Oracle's strategic approach to developing secure software depends upon building un-bypassable security into the database. Its security mechanisms are designed and tested to grant access to the appropriate users while keeping out hackers and other unauthorized users.
3. Secure Solutions. Oracle's industry-leading security features and solutions lend themselves to privacy-centric implementations.

Let's explore the first two strategic approaches in detail, then examine in detail the security features and solutions that lend themselves to privacy-centric deployments.

ASSURANCE

Where does one turn to validate the conflicting security claims from competing vendors? Independent evaluations against internationally-established security criteria provide assurance of vendors' security claims.

Security evaluations are carried out by independent, licensed and accredited organizations. Some evaluations are even industry standards; the International Common Criteria is ISO standard 15408. The evaluation process, from inception to certificate issuance, often lasts up to a full year. The evaluators not only examine the software design and code, they also consider process aspects, development, testing and production practices. Organizations who have undergone evaluations at a high level of assurance improve their coding, testing and software or hardware product as a result of completing the demanding process.

Assurance gained from independent evaluations is a cornerstone of product security, just as security is a cornerstone of privacy. Germane to Oracle Corporation's strategy with respect to security and privacy is the undertaking of independent security evaluations. The Oracle9*i* Database builds upon 15 independent security evaluations of its data server software. Nine of those evaluations have examined the security of the Oracle database, and the first was completed eight years ago, in 1994.[vii] No other database vendor approaches the number of evaluations that Oracle has, nor can they claim the years of experience from the efforts behind these evaluations.

The National Security Telecommunications Systems Security Policy number 11 (NSTISSP), in effect since July 2002, in essence states that any system involved in national security requires independent measures of assurance, such as a FIPS-140 certification or a Common Criteria (CC) evaluation. The US Federal government requires these measures of assurance in their most sensitive applications. The US government requirement for security evaluations underscores the importance of evaluations. Oracle is well-positioned to protect the security of national security data; it is as effective for protecting your users' confidential information.

Vendors who have not completed any evaluations can claim little objective assurance of the security implementations in the product. Evaluations are perhaps the most effective way to qualify a vendor's assertions about its security implementations because they supply independent evidence of properly implemented security against established criteria. Customers who choose an unproven database product can potentially suffer the consequences of a deployment lacking a basic principal of privacy: product security.

DATABASE-ENFORCED SECURITY

It would be difficult for Oracle, or any database vendor, to design software that adequately protects valuable information without properly securing the database itself. Because the database holds the most important of an organization's data, it is absolutely critical to protect this repository. The saying goes that implementing security outside of the product you are securing is like a bank locking the front door, but not the vault inside. The bank secures the vault because it is the money in the vault that it needs to protect. They layer on additional security mechanisms, but the most stringent is on the money itself. Likewise, you must put the most stringent protections on the data itself where it is stored. Additional safeguards should be used as well, but not securing the data in the database is a non-starter.

Oracle protects the data itself where it is stored—in the database. It protects data at a more granular level than any other vendor. Oracle9*i* provides a variety of security features, from user authentication to privilege management and row-level access control, which its customers leverage in their privacy-enabled deployments.

Hackers, and the threat of internal employees and users, pose a distinct threat to data privacy. Someone who hacks an application or otherwise gains unauthorized access to data may well access PII. It is therefore imperative that privacy-enabled businesses deploy software with security built-in, and, better yet, software with independent assurance of its security implementations.

Many Oracle competitors do not build substantive security into the database itself. This approach leaves customer data vulnerable to attack by a user who bypasses application-based security. The industry recognizes Oracle's stronghold in the security market, and Oracle's privacy-enabled database forms the backbone of its customers' privacy deployments.

LEVERAGING THE ORACLE9I DATABASE FOR PRIVACY

Given the close relationship between privacy and security, it is important to understand the features and functions of the products in which you store your customer's PII. As already established, it is crucial to safeguard the personally identifiable data stored in a database, and you can leverage Oracle9*i* Database solutions within your deployment as a

foundation for protecting the PII of your customers. The remainder of this paper identifies the key Oracle9*i* Database solutions that can be leveraged to protect the privacy of user's and consumer's PII.

AUTHENTICATION: WHO IS THE USER?

Because authentication is a primary element of security, it plays a role in privacy. Consider a healthcare provider who, as part of its HIPAA compliance, allows patients to check their own records for accuracy and disclosure purposes. First the user must prove her identity, beyond a doubt, to ensure that she is checking (and possibly updating) her own medical record and not another user's record.

The basis for system security is strong user identification and authorization. If you cannot establish, with certainty, who a user is, then it is difficult to ensure that users only have access to the data they need, but no more. Likewise, without the certainty of users' identities, it is impossible to hold users accountable for their actions. Authentication mechanisms identify users and verify the validity of their credentials.

Authentication is the essential first step in establishing who a user is, so that you then can determine the data he should be allowed to access. Without verifying the credentials of a user via authentication, an unauthorized user could gain access to data or resources that he should not.

Oracle9*i* supports a number of choices for user authentication. The most common method is the user password. Because weak passwords can be an easy entrance for hackers, Oracle9*i* provides built-in password management facilities to enable administrators to enforce minimal password length, ensure password complexity, and disallow passwords that are easily guessed words. With support for host-based authentication, Oracle provides the alternative using of the underlying operating system to authenticate users.

STRONG AUTHENTICATION AND SINGLE SIGN-ON

Strong authentication refers to any mechanism stronger than a password. Strong authentication mechanisms benefit the organizations that deploy them because these solutions are easy for the users—often as easy as a password—but even more secure. The benefit of using strong authentication is that it is harder to break than basic password authentication, and it provides higher assurance that the user is who she claims to be. As such, they help you to secure your assets, including PII.

Network authentication services, such as Kerberos, supply strong user authentication, as does the Internet-standard Remote Authentication Dial-In User Service (RADIUS). Two-factor authentication proves user identity based on something the user has (such as a smart card) and something she knows (a personal identification number or PIN), and is another popular means of strongly authenticating users. Oracle delivers strong authentication as part of the Oracle Advanced Security option. This database option also supports a Public Key Infrastructure (PKI) that uses industry-standard X.509 digital certificates for strong authentication.

Single sign-on (SSO) is the act of logging in once, then getting access to multiple servers or applications using a single authentication credential. Users employ a single enterprise username and password to connect to multiple databases applications.

Users with a single password tend to use better, harder-to-break passwords because they have only one to remember. Business benefits of single sign-on are the reduction in customer Support calls due to lost or forgotten passwords and increased security.

Oracle's support for Kerberos, digital certificates, and enterprise user security (detailed later) enable users to take advantage of single sign-on. SSO requires infrastructure to authenticate and manage permissions to distributed systems, while the user enjoys the ease of a single login. Some people consider SSO the "holy grail" of security with its combined ease-of-use, management and security benefits. Oracle customers use the database and Oracle Advanced

Security authentication and single sign-on methods—as well as Oracle9*i* Application Server http security, Java security and Single Sign-On for web-based applications—as part of their security and privacy solutions.

AUTHORIZATION: WHAT CAN THE USER DO?

Once you establish who a user is through authentication, you must determine what assets he is permitted to access and manipulate. Authorizations (namely, roles and privileges) determine what data a user should have access to and what types of operations he can perform on those objects. A user can only perform an operation on a database resource or object, such as a table or view, if an administrator or another user has authorized him to perform that operation.

Like authentication solutions, authorizations are a basic part of privacy deployments. For example, the US Department of Defense (DOD) healthcare system, which has 8.7 million beneficiaries, must comply with the DOD's well-established medical data privacy initiatives and now with HIPAA requirements. As a fundamental part of their privacy and security provisions, the DOD's healthcare system, called the Military Health System (MHS), relies on the Oracle Database for role-based security to limit data access to authorized users.[viii]

A privilege is an authorization to perform a particular operation. Without explicitly granted privileges, a user cannot access any information in the database. To ensure data security, a user should only be granted those privileges that he needs to perform his job functions, but no more far-reaching permission. This is known as the principle of "least privilege."

The Oracle database enables the grouping of individual privileges into roles. The collection of 'select' privilege on the orders table, 'select' and 'insert' privileges on the accounts table, and 'delete' privilege on the regional orders view might be grouped into the "sales" role. The administrator grants the sales role to any users who should have the rights to access the objects with the specified permissions. The next section discusses further controlling access within objects.

Oracle scales privilege management by leveraging Oracle Internet Directory (OID), an LDAP-compliant (Lightweight Directory Access Protocol) directory service, to centralize management of users and their authorizations across multiple databases. Oracle Internet Directory as the foundation for centralized management is further explained in the Identity Management discussion. Centralized privilege management provides the benefit of easier, consistent administration of users' rights and permissions from a single location. It provides security and scalability benefits, as well as a lower Total Cost of Ownership (TCO).

ACCESS CONTROL: WHAT CAN THE USER ACCESS?

The above examples illustrate object-level privileges, as they specify which database object a user may access. Oracle9*i* moves far beyond any other database vendor's access control solutions with support for highly granular access control within objects. Therefore, Oracle9*i* customers benefit from better security, the ability to build privacy-centric deployments, and lower TCO as a result of using these solutions.

VIEWS FOR ACCESS CONTROL

Views allow you to further limit the data a user can access within an object. A view is a subset of one or more tables (or views). You can define, for example, a view that allows a manager to view only the information in the customer table that is relevant to customers of her own department. The view may contain only certain columns from the base table, such as customer name, geographic region, sales rep, and contact information. Views can also limit the subset of the rows accessible in the base table, such as a view of the employee table which contains records for employees assigned to department 10.

While views can provide some level of access control within an object, they have limitations which make them less than practical for granular access control.

First, views do not scale well to enforce your security and privacy policies. For example, using views to restrict access to a school district's student records by school, is feasible if there are 12 schools in the district, and hence 12 views. But it may not be practical to use views to limit access when data must be shared across school districts. Managing thousands of the views, which are themselves objects, for every school and every district would be an administrative burden.

Second, a complex access control policy does not lend itself to views. For example, an access control policy "a user accessing the Employee table as a Payroll clerk through the Payroll application is allowed to see all employee information, including PII such as social security number, but only for employees in her division." This is probably not possible to express in a view, since you can't determine what application the user is accessing at the time you create the view.

Third, users with access to the tables your views are based upon can bypass security enforced in the views, which can violate privacy policies when the base tables contain PII. Applications may enforce security through views, but application users may need to run reports on the base tables. Users with privileges on base tables are able to bypass the security enforcement provided by views. Note that this is a general problem of embedding security in applications instead of enforcing security through database mechanisms, but it is exacerbated when security is enforced on views and not on the data itself. The privacy implications are enormous when the base tables contain PII.

Lastly, views for security can complicate administration of security policy. A security administrator cannot tell the difference between the parts of a view definition based on logical object definition, and those designed to enforce security. When a security policy is added, changed, or removed, it is difficult to determine what exactly to do with each view. An administrator cannot tell whether, by changing security policies through altering or dropping a view, whether she is breaking the application.

Oracle has developed a better way to enforce granular access control within the database in a scalable, secure, and lightweight way.

VIRTUAL PRIVATE DATABASE

The Virtual Private Database (VPD) enables, within a single database, per-user or per-group data access with the assurance of data separation. VPD is the aggregation of server-enforced, fine-grained access control, together with a secure application context in the Oracle database. VPD is designed for transparency, performance, scalability, and above all, security. This solution is unmatched by any other vendor, and the transparent row-level granularity makes it ideal for privacy-centric applications.

By dynamically appending SQL statements with a predicate (a "where" clause), VPD limits access to data at the row level and ties the security policy to the table (or view or synonym) itself. Security is stronger because it is enforced by the database, no matter how a user accesses data; a user running a query tool or report writer cannot circumvent the security. Non-bypassable security can enforce privacy policies on the data itself, which is critical for keeping PII private.

Many Oracle customers, representing a vast number of industries, use Virtual Private Database technology to separate data by customer, by organizational unit, by region, and so forth. They use VPD as part of their compliance with privacy regulations and corporate policies. VPD is used to enforce business policies requiring that employee personal information, medical records, and student records remain confidential.

Because the technology enables Oracle customers to consolidate data into one very large database with the guarantee of data separation, rather than running dozens of separate instances, it lowers the cost of ownership. Another benefit of building security into one central database is the enforcement of international privacy policies. It allows for the PII of one country's citizens to be protected just as judiciously as any other country's citizens—all in one location. Customers enjoy the benefits of building security once, in the database, and certifying the core security code in the database, not multiple applications.

Where privacy is essential, the Virtual Private Database is indispensable. For example, a consumer bank in Asia might offer an online banking service in which its customers perform online transactions and check their account balances. It is vital that the user sees only her own account balances, but no other customer's account information. The bank that uses Virtual Private Database can easily scale to tens of thousands of users accessing one large database, with the assurance of complete data separation, as well as the benefit of straightforward database administration. As an additional feature, the banking application can transfer monies directly from the user's bank account to another bank (for example, to pay a credit card bill). With VPD, the partner banks can share the data without sharing such personal information as account balance or balance history.

Virtual Private Database deployments rate high on the list of Oracle customer's security and privacy implementations. The utility of VPD reaches well beyond financial services, with a neat fit into the ASP market, healthcare, in government deployments worldwide, and data warehouses. It is a driver for web-based e-commerce applications from retail to education markets.

Label-Based Access Control

Built on top of VPD, Oracle Label Security enforces label-based access control for row-level security. Oracle Label Security is the security option for the Oracle9*i* database that mediates access to data by comparing a sensitivity label on a piece of data with label authorizations assigned to an application user. Such access mediation allows data to be separated into different sensitivities within a single database. Oracle Label Security is scalable, secure, and it is enjoying commercial success with privacy-centric customers.

Labels are used extensively in commercial and government organizations. Examples of labels include: internal, confidential, sensitive::human resources, and internal::Acme California for the Acme Corporation with a branch in California. Oracle Label Security uses an Oracle-supplied security package to mediate access to data rows, and no coding or PL/SQL software development is required, making it easy-to-use and manage.

Label-based access control lends itself to privacy, perhaps more than any other element of Oracle's security solution set. With Oracle Label Security, only those users with appropriate "clearances"—access to data with specific labels—can access or modify privacy-sensitive data. This technology grew out of the need for a hierarchical representation of access control. The power of Oracle Label Security emerges in privacy-sensitive implementations, for example in a healthcare application in which a patient's diagnosis is labeled "confidential::physician." Because of the label, no one apart from the individual authorized at the confidential level and the physician group can access the patient's diagnosis.

Another fitting privacy example using Oracle Label Security involves the education market. Students' state test scores must be protected so that the administration of one school can see its own test scores, but not those of other schools in the district. A hierarchical requirement complicates matters, for the school district's superintendent needs district-wide access. Student records can be labeled "sensitive:testscore:JFK High." The sole user with access to the entire set of student records is the superintendent. The JFK High School principal sees his school's test results, but not those of the other high schools. Likewise, principals from other schools are restricted from accessing JFK's test scores. The student's right to privacy is intact, teachers and administrators can efficiently do their jobs, and security maintenance is kept low for the database administrators.

SECURE APPLICATION ROLE

A long-standing security problem has been preventing users from bypassing application logic and accessing data directly. In web-based applications, in particular, it may be undesirable to allow users direct access to data. To date, this has been a very difficult security problem to solve because there has been no secure way to validate which application is used to access data. That is, a malicious user could write a program that appears to be a valid human resources application, but, in fact, is not.

Oracle9*i* addresses this challenge through a secure application role: a role implemented by a package. Without secure application role, developers have devised schemes like hard-coding passwords into the application accessing the database or obscuring database information so that a user who attains direct access has to piece together the meaning of the data. Security edicts recommend against both of these practices.

The package that sets the secure application role can perform any desired validation to ensure that the appropriate conditions are met before the user can exercise privileges granted to the role in the database. For this, it can use a number of pre-defined attributes as part of its access control decision, such as IP address, current user, proxy user, external name, and territory. The database ensures that it is only this package implementing the role that determines the correct access conditions. Without secure application role, privacy-relevant personal data may be at risk whenever a user finds a way around the application and into the database itself.

As an example, consider a government agency (in any country around the world) that uses application roles to prohibit their tax clerks from directly accessing database-stored tax records with taxpayers' PII. The only way a tax office worker can use his tax clerk permissions is by connecting to the database through the web-based Income Tax Processing application. The application uses an associated role of 'tax_clerk'—a secure application role that can only be implemented through a package owned by the application. Thus, the taxation office worker can never access citizens' records any other way than through the proper application.

Secure application role enhances the native authentication and fine-grained access control to prevent users from assuming any privileges unless the correct access conditions are met. This feature solves a very difficult security and privacy issue and supports secure web-based application data access.

The benefits of secure application role are the improved security and unique ability to tie security enforcement to a particular application. Secure application roles help you to run a secure three-tier environment where you are assured that users cannot bypass applications. This solution represents another way in which Oracle9*i* helps you protect PII when it is stored in the database.

IDENTITY MANAGEMENT

Oracle leverages Oracle Internet Directory, the LDAP-standard directory, for centralized management in the Oracle environment. The Oracle9*i* Database harnesses its power to centrally manage users, their authentication credentials and their authorizations. The Oracle Internet Directory serves as the centerpiece for large-scale deployments where centralized administration is imperative. Oracle has directory-enabled the various components of its product stack to take advantage of the scalability, management and security of Oracle's LDAP directory service.

The Oracle Internet Directory unites user definitions in Oracle9*i* Application Server Single Sign-On and Oracle9*i* Database enterprise users. Customers leverage the unification for something they have never been able to accomplish before—provision and manage a single user identity. This user identity is, in turn, used by applications, application server components, database access, and so on.

For central control with Oracle's Delegated Administration Service, administrators use a browser-based application to create, update, suspend or delete user information stored in the directory. Likewise, end users employ the Delegated Administration Service to modify data about themselves. Centralization is the key to tracking and managing user's

authorizations. Centralization allows you to manage privacy preferences and exert central control over w[ST1]ho is authorized to access PII.

The single user identity, centralized privilege management and centralized administration are integral parts of building an infrastructure for privacy. It is far easier to ensure that privacy preferences are enforced if there is a common notion of the user. If the privacy policy changes, you can manage access rights centrally, thereby you can easily change rights as privacy policy evolves. Additionally, you gain the cost savings inherent in self-service and consolidated administration.

For example, compare two insurance companies working to protect the privacy of personal data they collect, both running dozens of applications and databases containing personal customer data. Company A employs a DBA per database and several application administrators to assign, manage, and revoke authorizations daily to protect customers' PII. Every administrator repeats the process, customizing it for his or her system. This represents management-intensive approach to privacy protection through authorization management and access control. Company B has an identity management solution. One or two administrators centrally manage all users' authorizations in the directory. Their enterprise-wide authorization management maps to database- and application-specific roles on each of its databases and applications. Company B achieves lower management costs, and it is likely to be more successful at controlling access to patients' PII.

PROTECTING DATA IN TRANSIT

Encryption tops the list of solutions employed to address traditional security threats. Whenever handling confidential data, it is important to encrypt packets flowing over the network and Internet as well as especially sensitive data in the database.

ENCRYPTION IN THE DATABASE

Highly-publicized compromises of credit card numbers and regulatory measures for protecting personally identifiable information have prompted many organizations to consider additional means of protecting confidential and especially sensitive data (e.g., national identifiers, credit card numbers) held in databases. Above and beyond other security mechanisms, one can obtain an additional measure of security by selectively encrypting sensitive data before storage in the database.

Oracle provides a flexible interface to encrypt especially sensitive data in the database server. Oracle has been enhancing the database encryption solution over the years, adding in Triple-DES encryption and MD5 cryptographic checksums, and Oracle9*i* provides a Federal Information Processing Standard (FIPS)-certified Random Number Generator. In the current release, Oracle provides DES (56-bit) and Triple DES (112- and 168-bits) in an encryption toolkit package that enables applications to encrypt data within the database. Customers actively protecting sensitive and/or personal data use these encryption interfaces both to comply with regulations and for ethical reasons—to efficiently safeguard such data.

NETWORK ENCRYPTION

It is perhaps even more important to encrypt data passing over a network where it is not protected by access controls, authorizations, and other security controls in the database. It is important to encrypt network communications in order to keep anyone from viewing, modifying or stealing data when it is sent over the network.

Oracle Advanced Security protects all communications with the Oracle Database. To encrypt network traffic, it provides Secure Sockets Layer (SSL), the Internet standard. Oracle Advanced Security also offers "native encryption" of Net8 with: the Advanced Encryption Standard (AES), DES, Triple DES, and RC4.

Many of these cryptographic modules have undergone the laborious certification process to obtain FIPS 140-1 Level 2 compliance, providing assurance of the implementation—down to the randomness of key generation.

To prevent modification or replay of data during transmission, Oracle uses an MD5 or SHA-1 message digest included in each network packet. Oracle's encryption and data integrity capabilities protect Oracle clients and middle tier servers in communications over Net8, Net8/SSL, IIOP/SSL, and also secure Thin Java Database Connectivity (JDBC) clients. In short, Oracle provides a variety of ways to encrypt communications over all protocols with any database communications. Wherever the database runs, the network traffic can be protected with encryption. Whenever sensitive data is sent over the network, Oracle can protect it.

AUDITING: MONITORING & ACCOUNTABILITY

Auditing is a passive, albeit important, security mechanism and a key enabler for privacy. A critical aspect of any privacy policy is maintaining a record of system activity to ensure that users are held accountable for their actions. To address this requirement, Oracle9*i* provides extensive audit facilities.

Oracle audits database activity by statement, by use of system privilege, by object, or by user—whether the operation is successful or unsuccessful. Audit records can be stored in a database table, making the information available for viewing through ad hoc queries or any appropriate application or tool, or combined with operating system audit trails on selected operating systems, for security and ease of management. Oracle implements auditing efficiently; statements are parsed once for both execution and auditing. For DBA accountability, Oracle can audit all SYS operations to the operating system, for review by a security administrator or auditor.

Additionally, Oracle makes use of database logs to capture operations performed by administrators and every user. Oracle captures all changes to the database, and they can be queried using the LogMiner utility. Thus, customers get the benefit of auditing without any additional overhead. Since the database must be recoverable, the logs are always available; Oracle does not drop records of any changes made to it. Auditing is implemented within the server itself, with a variety of audit options, allowing customers to record specific database activity without incurring the performance overhead that more general auditing entails.

Auditing can be used for investigative purposes as well. For example, a particular doctor may be attempting to look at the charts of patients she is not treating. Whether or not the doctor is able to retrieve the records, Oracle9*i* can track the doctor's behavior more closely—by auditing successful and unsuccessful attempts to access other patients' records.

FINE-GRAINED AUDITING

In general, if not done carefully, the sheer volume of audit logs can make finding suspicious activities like searching for a needle in a haystack. Auditors and security administrators aim to reduce the amount of data logged but capture all relevant data. Granular auditing dramatically reduces the amount of data captured and hones in on the sensitive data that must be audited. Oracle9*i* Database expands upon the above auditing facilities with something unique in the industry, Fine-grained Auditing.

Fine-grained Auditing allows organizations to define audit policies, which specify the data access conditions that trigger the audit event. Cutting down on audit logs allows you to hone in on suspicious activities. Administrators can use a flexible event handler to notify them that the triggering event has occurred. The event handler sets a triggering audit event to be written to a special audit table for further analysis, or it could activate a pager for the security administrator. As such, Fine-grained Auditing can be an investigative tool.

Fine-grained Auditing employs "relevant column" auditing to hone in on particularly sensitive columns, such as national identifiers, which your corporate policy may define as privacy-relevant. The access control policies can

protect against an employee viewing another employee's records, and auditing can monitor that the access control is properly implemented, specifically when a user attempts to access data in the column holding national identifiers.

In general, auditing does not capture the data returned to the user because audit logs would become too large. Fine-grained Auditing captures the exact SQL text of the audited statement, and when used in combination with Oracle's Flashback Query feature, you can recreate the exact records returned to a user. This combination defends against the user who tries to subvert the auditing mechanisms by issuing hard-to-detect queries that may hide the intent of the query.

The scope and granularity of auditing features shipped inside Oracle9*i* Database are key for privacy-enabled environments. Customers with a need to log and inspect database access without taking on high overhead, those with corporate auditing mandates, and those with industry regulations (such as HIPAA in health care) use these advanced auditing capabilities innovated by Oracle9*i*.

FEATURE SUMMARY

Oracle builds advanced features that allay your customers' concerns about the threats to their PII, from overly-broad employee access, the threat of hacker intrusion, and simple mismanagement of data. These advanced features, including row-level security, fine-grained auditing, and centralized administration, meet or exceed customers' privacy requirements. Along with adjusting policies and procedural operations effectively for privacy, you can achieve privacy compliance by implementing these solutions in your systems.

CONCLUSION

Privacy protection is not just a simple matter of running privacy-enabled software; choosing secure IT products is but the first step towards effective privacy management. Operational, organizational, and policy decisions greatly affect your privacy qualifications. While privacy regulations might appear to be a compliance burden that distracts you from your objective of running an efficient business, in fact, the protections you may have to implement for compliance with industry- or country-specific regulations can help your business burnish your reputation and increase customer satisfaction. Such protections help you to run a tighter, more secure IT infrastructure. Your business benefits from better security, more scalable user access management and lower cost of ownership, while your customers reap the rewards of well-protected personal data.

---

[i] http://www.ftc.gov/privacy/
[ii] http://www.epic.org/privacy/bill_track.html
[iii] http://europa.eu.int/comm/internal_market/en/dataprot/
[iv] http://www.export.gov/safeharbor/
[v] http://www.export.gov/safeharbor/sh_overview.html
[vi] http://www.senate.gov/~banking/conf/ and http://www.epic.org/privacy/glba
[vii] The Oracle RDBMS has undergone and completed the following evaluations:
Common Criteria - Three Oracle RDBMS evaluations completed at level EAL4
ITSEC - Three Oracle RDBMS evaluations completed at level E3/F-C2
TCSEC - One Oracle RDBMS evaluation completed at C2 level
Russian - One Oracle RDBMS evaluation completed at level IV
Russian - One Oracle RDBMS evaluation completed at level III
[viii] http://www.iw.com/magazine.php?inc=100102/10.01.02bizlab.html