

# Role Based Authorization as a Tool for Privacy and Anonymity

Douglas C. Sicker  
Department of Computer Science  
Interdisciplinary Telecommunications Program  
Computer and Communications Security Center  
Center for Science and Technology Policy Research (Faculty Affiliate)  
University of Colorado at Boulder  
Boulder, Colorado 80309  
303-735-4949  
douglas.sicker@colorado.edu

*The advent of the information age has brought a proliferation in the amount of information that is available and an increase in accessibility to such information. As we rely more heavily on networks as a means of communicating, we must increasingly consider how these networks store and distribute this information. Aside from the problems that arise in managing the security of large diverse systems, we must also consider the implications of distributing personally identifiable information across such systems. For example, both web browsing and voice over internet communications processes include considerable amounts of personally identifiable information about the user. For some, the distribution of (and access to) this personal information is of no consequence; however, for others, this is tantamount to an invasion of their privacy. Some of the issues associated with the distribution of this information arise out of the identity, authentication and authorization models that have been defined for these services. Many of the existing models rely heavily on identity information that readily links back to an individual (i.e., an individual's name as their login). Further, many models do not provide support for privacy or anonymity, nor do they provide granularity in terms of what information might be released to whom and methods of controlling such release.*

*To address these problems, various groups are working on new role-based authorization (RBA) models. The value of a RBA approach is that the user asserts a 'role' rather than a typical identity when requesting a service. In this way, the user can maintain some level of anonymity and privacy. However, the actual identity of the user may still be maintained by the local domain, thereby addressing possible repudiation and legal concerns (i.e., CALEA). These RBA systems also allow the user to determine the amount and type of information released about that user. This granularity of control can be used to adjust the level of anonymity associated with a communication session. For example, a user may want one session to be anonymous and the next not.*

*In this paper, we will begin by providing some relevant technical background material and loosely define two rather contentious terms, privacy and anonymity. We will then briefly describe the RBA models under development, including the motivation of these models. We will demonstrate how these models can be used to provide privacy and anonymity. Next, we will consider the policy implications of RBA models, particularly as it relates to US federal law and policy. We will end by considering how privacy, anonymity and law might co-exist.*

# 1. Introduction

“Privacy, particularly in the area of communications, is a well established policy and objective of the Communications Act. Thus, any threatened or potential invasion of privacy is cause for concern by the Commission and the industry. In the past, the invasion of information privacy was rendered difficult by the scattered and random nature of individual data. Now the fragmentary nature of information is becoming a relic of the past.”<sup>1</sup>

This quote from the Computer Inquiry (circa 1966) is still astonishingly relevant today. However, it is unlikely that the writers of these words had any inkling of just how dependent our society would become on computers and the networks that connect them. Furthermore, it is not likely that the writers perceived just how readily available personal information would become on these networks. Nonetheless, the recognition of privacy as a policy objective remains.

The advent of the information age has brought a proliferation in the amount of information that is available and an increase in accessibility to such information. As we rely more heavily on networks as a means of communicating, we must increasingly consider how these networks store and distribute this information. Aside from the problems that arise in managing the security of large diverse systems, we must also consider the implications of distributing personally identifiable information across such systems. For example, both web browsing and voice over internet communications processes include considerable amounts of personally identifiable information about the user. For some, the distribution of (and access to) this personal information is of no consequence; however, for others, this is tantamount to an invasion of their privacy. Some of the issues associated with the distribution of this information arise out of the identity, authentication and authorization models that have been defined for these services. Many of the existing models rely heavily on identity information that readily links back to an individual (i.e., an individual’s name as their login). Further, most models do not provide support for privacy or anonymity, nor do they provide granularity in terms of what information might be released to whom and methods of controlling such release.

To address these problems, various groups are working on new role-based authorization (RBA) models. The value of a RBA approach is that the user asserts a ‘role’ rather than a typical identity when requesting a service. In this way, the user can maintain some level of anonymity and privacy. However, the actual identity of the user is still maintained by the local domain, thereby addressing possible repudiation and legal concerns (i.e., CALEA). These RBA systems also allow the user to determine the amount and type of information released about that user. This granularity of control can be used to adjust the level of anonymity associated with a communication session. For example, a user may want one session to be anonymous and the next not.

In this paper, we will begin by providing some relevant technical background material and loosely define two rather contentious terms, privacy and anonymity. We will

---

<sup>1</sup> Notice of Inquiry, In the Matter of Regulatory and Policy Problems Presented by the Interdependence of Computer and Communication Services and Facilities, Docket No. 16979, 8 R.R. 2d 1567, 1572 (1966).

then briefly describe the RBA models under development, including the motivation and rationale of these models. We will demonstrate how these models can be used to provide privacy and anonymity mechanisms. Next, we will consider the policy implications of RBA models, particularly as it relates to US federal law and policy. We will end by considering how privacy, anonymity and law might co-exist.<sup>2</sup>

## 2. Terms of Contention

In this section, we examine two rather contentious and misunderstood terms, privacy and anonymity. With the advent of the information society, these terms have become closely coupled. The objective of this section is less about actually defining the terms, but rather providing some basic understanding and appreciation of their complexity.

### 2.1. *Privacy*

The popular press is filled with accounts of battles between individuals, companies, and governments regarding stances on privacy in the electronic world. Many companies are seeking to expand their ability to capture information in the electronic world, which is certainly changing the face of privacy as a space. Governments, in the wake of the recent rise in terrorist related casualties, are desperately seeking means to protect the interests of the countries they represent. These changes are reshaping society in overt and subtle ways, and have varying implications on privacy.

This raises the question, what is privacy? In the landmark case *Olmstead v. U.S.*, Justice Brandeis defined privacy as, “The right to be left alone –the most comprehensive of rights, and the most valued by a free people.”<sup>3</sup> Webster’s Dictionary defines privacy as “freedom from unauthorized intrusion.”<sup>4</sup> Taken to extremes, perfect privacy is conceptually feasible, though impractical, as it would require isolating one’s self from the world. Beyond such simplistic definitions, it seems prudent to shy away from making definitive statements, in that privacy has a very subjective nature. Privacy advocates, however, often appear to treat the subject in a similarly simplistic manner. Statements are made claiming some action will result in a loss of privacy. Yet, defining that loss is often avoided or subjectively stated. [Giacomoni]

Privacy is a function of the prevailing culture, social context, political context and the individual ideals. For example, national boundaries can proxy the prevalent political and cultural ideals, whether by choice or force. Germany’s present deferral of privacy decisions to the individual is in sharp contrast to the Chinese model where all privacy decisions are subjugated to the government. Both contrast to the current policy in the United States, where privacy is at the mercy of its market economy. As presciently foretold in the *Computer Inquiry*, moving from the physical world to the electronic one, we find many of the physical world rules to be less than clear. Concerns widen from purely physical equivalents (such as unauthorized distribution of personal photos), to include more intimate details of one’s self. These changes speak in a different way, for in an electronic world one’s identity is captured easily in reproducible bits of information. [Giacomoni]

---

<sup>2</sup> I would like to thank Lisa Blumensaadt for her invaluable assistance on this paper.

<sup>3</sup> *Olmstead v. U.S.*, 277 U.S. 438, 1928.

<sup>4</sup> Webster’s New World Dictionary, College ed.

Given the above discussion, we see difficulty in defining privacy without tying it to a specific attributes and individuals. In the anonymity discussion that follows, we describe a means of providing this connection.

## **2.2. Anonymity**

Systems that allow users to control the amount of personal information (IP address, email address, physical address, real name, etc.) revealed to different entities on the Internet can be used to reclaim an individual's online privacy. We consider two forms of online privacy, anonymity and pseudonymity (although in practice both are normally referred to as anonymity). A system that provides anonymity hides the user's identity unless the user chooses to reveal their identity. Pseudonymity is a type of anonymity; however, with pseudonymity the user maintains one or more distinct identities (pseudonyms, or nyms) that are not connected to the user's physical identity.<sup>5</sup> Most systems use some secret that only the user who created the nym knows to ensure that people with whom the user interacts using a given nym can be assured that, although they do not know the physical identity behind the nym, it is in fact the same person each time. However, more than one person may "share" a single nym simply by sharing the secret. In contrast, anonymous systems that provide strong or unlinkable anonymity do not leave any persistent information that lets someone link any transaction to another transaction performed by the same user. [McCoy]

Anonymity is not an all or nothing proposition. There are different levels of anonymity. Ian Goldberg came up with the idea of a "nymity slider" which is likely the most useful way of thinking about this situation. [Goldberg] He divides digital identity into four general points on a continuum. The nymity slider starts with "verinymity," which is essentially no anonymity. At the other end of the slider is "unlinkable anonymity," a term for the kind of completely anonymous identity you have when, for example, you use cash to make a one-time purchase from a stranger. Unlinkable anonymity is completely anonymous because it is the single appearance of an identity and is never used again. Of course, between these extremes lie other levels of anonymity. [McCoy]

Now that the varying degrees and properties of anonymity have been discussed, one question is; should people be able to use the Internet anonymously? Many people argue that only those who have done something wrong feel the need to remain anonymous and people that have done nothing wrong have no need to hide. This follows that only criminals and degenerates have a need for anonymity. However, keep in mind the need for anonymous speech is an arguably a component of the right of free speech. The Federalist Papers (one of the Nation's most influential political tracts) were published anonymously as many controversial documents have been since. Therefore, it is worthwhile to consider how some level of anonymity might be maintained on the network.

## **3. Technology of Role Based Authorization (RBA)**

In this section of the paper, we briefly describe some relevant background material. We begin by discussing the notion of a federation, which can be described as a mutual

---

<sup>5</sup> A user must take care that if they maintain multiple nyms that these nyms cannot be linked to a single person by use of stylometry, a linguistics technique that can be used to link documents to the same author using vocabulary, common misspellings, etc. This attack was proven effective in [Rao].

agreement between realms explicitly for the sharing of resources. We then describe the notion of role-based authorization.

### **3.1. Federation**

Network resources exist as islands, controlled and maintained by a network authority, typically a network administrator. This control of resources includes access control mechanisms in the form of authentication and authorization. A problem arises when someone from outside of a particular realm wishes to access a resource for which he/she has no authorization. Resources may be perceived as ranging from public to highly restricted, which suggests the need for granularity of access control.

One means of providing this authorization is through the development of an agreement between the user and the realm in which the resource exists. The problem with this approach is that the network authority controlling the resource must now maintain information, such as a username and password, for each foreign user. This can quickly become a burden for the network authority as the number of foreign users increase. An alternative is to create a mutual agreement between realms, explicitly for the sharing of resources between realms. This is the federation, where access is controlled jointly by adopting certain trust agreements between realms. For example, domain A and domain B could agree that users from either domain could access databases from the other's domain. In order to secure such a federated model, some type of cross-domain authorization is necessary. Cross-domain authorization entails a user in one domain being authorized by an agent in another domain.

This authorization can be done in a number of ways. In one approach, the authorization decision cannot be made by this agent without accessing the user's information. The user must trust the sharing of identifiable user information to access the remote resource. This raises several opportunities to exploit that user's privacy. An alternative to the simple sharing of user information between domains would be to assert an attribute (e.g., authority level such as professor/researcher/student etc.) and have this attribute examined by the authority of the remote resource. The remote authority may examine the authenticity of this assertion and make a decision regarding access.<sup>6</sup> Thus, delegation is practiced with each network domain in control of the information of its users. This reaffirms the general practice of network administrators to keep local information within the domain. This also reduces the burden on administrators of resources that are shared across domains. They need not maintain a separate access control list for each remote user and the remote user is exposing less information about itself across a network. SAML is one example of a protocol that provides a framework for such a secure assertion of user information across domains. A secure federated model, thus, brings together parties with common interests while offering them protection at different levels among themselves and from others. [Sicker03a]

### **3.2. Role-Based Authorization**

As indicated above, one way of forming a federation is to assert an attribute and have this attribute examined by the authority of the remote resource. Role-based authorization (RBA) entails just such an assertion by an authorization service of attributes associated with an identity. These attributes describe the 'role' or 'roles' of the identity in question – facts

---

<sup>6</sup> This could be done with various cryptographic techniques, which are outside the scope of this paper.

about the principal corresponding to that identity. For example, a given principal might be a faculty member at a university. An assertion for that principal's identity might state that they have the 'role' of a faculty member. This allows role-based authorization to offer a very compelling privacy and anonymity solution. Identity becomes one more attribute of an assertion that may or may not be shared with various destinations. [Peterson03a]

A question worth asking is, why bother with this process? Authorization mechanisms require an authorizing agent to query some type database to ascertain the privileges of the concerned user. However, in a cross-domain scenario, this requirement may become burdensome. Firstly, given the number of users in the various domains, the databases would be unmanageably large. Secondly, users and system administrators alike would be reluctant to have sensitive user information stored in so many different locations. This necessitates a new mechanism to effectively handle cross-domain authentication and authorization. Role-based authorization, while not a new concept, is quickly gaining in popularity. A role-based security policy allows authorization decisions to be based on a role that the user asserts, rather than on his or her identity. [Ferraiolo] Role-based authorization essentially allows for more granularity in the authorization process, because one can choose what information to assert, and it considerably simplifies the tasks of network administrators since they no longer have to maintain accounts for foreign users. By basing authorization decisions on the functions or "roles" of the users, complex access control lists are no longer needed for every resource. All that is required is a set of simple mappings containing the various roles and their respective privileges.

#### **4. Role-based Service Models**

In this section of the paper, we present two RBA models; Shibboleth (for web services) and RBA enabled SIP (for voice services). Security Assertion Markup Language (SAML)<sup>7</sup> forms the basis of these two role based services. SAML is "an XML-based framework for exchanging security information. This security information is expressed in the form of assertions about subjects..." [SAML] Essentially, SAML allows assertions to be conveyed containing information about authentication acts performed by subjects, attributes of subjects, and authorization decisions (previously made) about whether subjects are allowed to access certain resources.<sup>8</sup>

##### **4.1. Web Services**

Shibboleth is an Internet2 project developing architectures and technologies to support inter-institutional sharing of web resources that are subject to access controls. For

---

<sup>7</sup> The protocol, consisting of XML-based request and response message formats, can be bound to many different underlying communications and transport. OASIS currently defines one binding; SOAP over HTTP, which forms the basis on Shibboleth (discussed in the next section of this paper). [SAML]

<sup>8</sup> Assertions can convey information about authentication acts performed by subjects, attributes of subjects, and authorization decisions about whether subjects are allowed to access certain resources. Assertions are represented as XML constructs and have a nested structure, whereby a single assertion might contain several different internal statements about authentication, authorization, and attributes. Assertions are issued by SAML authorities. An assertion is a package of information that supplies one or more statements issued by a SAML issuer. SAML allows issuers to create three different kinds of assertions: authentication assertion, authorization decision assertion and attribute assertion. SAML assertions/artifacts, protocol requests and protocol responses can be embedded in other structures for transport. The specification for the bindings and profiles provides a framework for this embedding and transport in SOAP messages over HTTP. [Mishra]

example, when a user in one institution tries to access a protected resource at a remote institution, attributes about that user can be made available to the remote institution, which can be used to make an authorization decision about that user. Shibboleth also allows users to determine what information is released to a destination site. Specific to our discussion, Shibboleth allows users to restrict the release of a user's name or other privacy related information.

#### **4.1.1. Operation**

Envision a typical web browsing session, where a user wishes to access a resource from a remote domain. In this scenario, the user would select a URL associated with that resource. However, before the web resource is delivered, a number of Shibboleth steps must first occur. The user's request is intercepted at the remote domain by a Shibboleth process that determines (through a series of steps) whether that user should be allowed to access the particular resource.<sup>9</sup> An important element of the Shibboleth architecture is the component that releases information about users, the Attribute Authority (AA). Each origin site (i.e., a site with administrative authority over users who access resources at remote providers) has its own AA. The AA's job is to provide attributes about a user to a resource provider. However, the AA also has the responsibility of providing a means for users to specify exactly which of their allowable attributes is sent to each site they visit.<sup>10</sup> For more details on the operation of Shibboleth, we refer the reader to [Shib].

#### **4.1.2. Privacy and Anonymity**

One difference between Shibboleth and other efforts in the access control arena is Shibboleth's emphasis on user privacy and control over information release. Shibboleth is a system for securely transferring attributes about a user from the user's origin site to a resource provider site. Again, Shibboleth allows users to determine what information is released about the user and to which site. Thus, the job of balancing access and privacy lies ultimately with the user, where it belongs. Shibboleth also keeps information local, meaning that a user does not have to worry (as much) about who has access to their user information and browsing behavior.

### **4.2. Voice over IP Services**

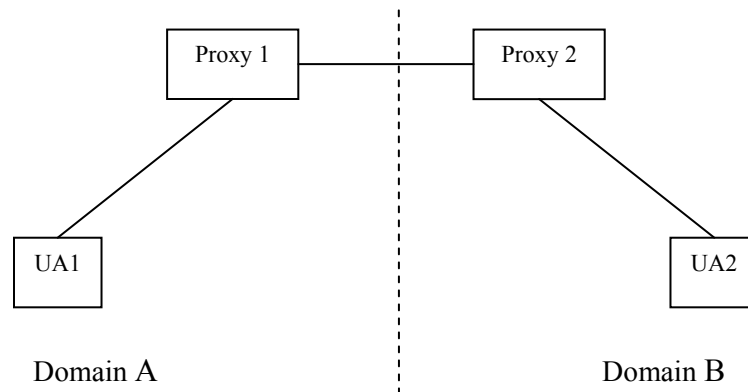
SIP can be thought of as a signaling service for voice over internet services, much like the Signaling System 7 is the signaling service for the PSTN. More formally, SIP is a protocol used for locating endpoints, and subsequently inviting these endpoints to a session. It operates by exchanging request messages called 'methods' and responses to these methods. SIP agents reside as software inside your PC (or in an IP phone). These agents work together with other software and hardware in your PC to provide telephone and other services. A SIP network essentially consists of software-based user agents (again, residing in your PC), which combines a User Agents Clients (UAC) that initiate requests and User Agent Servers

---

<sup>9</sup> This is an grossly simplified description of the Shibboleth process. For example, the design includes extensive security mechanisms to protect resources and information transmitted on the network. For a more thorough technical description, see [Shib].

<sup>10</sup> The Handle Service (HS) is another component of Shibboleth that resides at the origin site. It is a web-based service that creates "handles" for attribute queries of a user without revealing the users identity, thus guarding the user's privacy. This handle is then used to obtain the attributes of the user requesting access.

(UAS) that reply to these requests. SIP proxies (within the network) serve to assist the User Agents (UA) in completing the call by providing such functions as message routing and security. (See figure 1) While this is an oversimplification of SIP, it should suffice for the discussion that follows (a detailed explanation can be found in [Rosenberg]).



**Figure 1 SIP trapezoid**

#### **4.2.1. Operation**

In this section, we describe an RBA extension to SIP. Referring to the above diagram, UA1 attempts to initiate a session (a “call”) with UA2 in a different domain by sending an INVITE message (a request to begin a session). Proxy1 in the local domain intercepts this INVITE and initiates a process, which eventually results in the attributes (describing the roles) of the user being transferred to the remote domain in the form of SAML assertions. The remote domain (possibly Proxy2 or UA2) examines these assertions and makes an authorization decision based on the attributes of the user of UA1. If the user is authorized to initiate the session, then the INVITE is forwarded to UA2. On receiving the INVITE, UA2 responds with an OK if it wants to set up a session with the caller at UA1 and the call is completed according to the SIP specification [See Rosenberg]. For tracking authentication, we define an abstract entity, an Authentication Service, which also performs the function of generating and storing SAML assertions, packaging them into the appropriate form for transport across to the remote domain, and, on the target side, processing them to make authorization decisions. The AS is defined as a logical entity, likely associated with a proxy.

#### **4.2.2. Privacy and Anonymity**

As described earlier, role-based authorization entails an assertion of attributes associated with an identity by an authorization service. These attributes describe the 'role' or 'roles' of the identity in question - facts about the principal corresponding to that identity. For example, a given principal might be a faculty member at a university. An assertion for that principal's identity might state that they have the 'role' of a faculty member. When a UAS receives a request with this role assertion, it can make an authorization decision based on whether or not faculty members are permitted to make the request in question, rather than just looking at the identity of the UAC and trying to discover whether they are a faculty member through some external means. Thus, these assertions allow a UAS to authorize a SIP request without having to store attributes associated with the identity of the UAC itself.

In fact, when role-based authorization is used, an assertion can be presented to a UAS instead of the identity of the UAC user. In many cases, the UAS has no need to know who, exactly, has made a request - knowing the identity is only a means to the end of matching that identity to policies that actually depend on roles. This fact allows role-based authorization to offer a very compelling privacy and anonymity solution. Identity becomes one more attribute of an assertion that may or may not be shared with various destinations.

Supplemental authorization information might allow the UAS to implement non-identity-based policies that depend on further attributes of the principal that originated a SIP request. For example, the mere fact that a UAC has been authenticated by a UAS doesn't mean that the UAS will grant the UAC full access to its services or capabilities - in most instances, a UAS will compare the authenticated identity of the UAC to some set of users that are permitted to make particular requests (as a way of making an authorization decision). However, in large communities of users with few pre-existing relationships (such as federations of discrete service providers), it is unlikely that the authenticated identity of a UAC alone will give a UAS sufficient information to decide how to handle a given request.

Role-based authorization depends on an authorization service that is trusted by the UAC and the UAS. For that reason, authorization services are most applicable to either single domains, or federated domains that have agreed to trust one another's authorization services. This could be common in academic environments, or business partnerships that wish to share attributes of principals with one another. Some role-based authorization architectures have been proposed to provide single sign-on services, such as the Liberty Alliance. [Liberty]

## 5. Legal and Policy Considerations

In this section, we first describe the relevant law that does (or could) apply to the topic at hand. We then examine how the RBA voice over internet approach might fit this model. It is our contention that applying an RBA approach will solve some existing legal and technical issues.

### 5.1. The Law

The Communications Assistance for Law Enforcement Act (CALEA)<sup>11</sup> is congressional legislation written to support previous wiretap and surveillance laws in light of technological advances.<sup>12</sup> CALEA requires carriers to design or upgrade their equipment to support lawfully authorized Law Enforcement Agency (LEA) electronic surveillance under, for example, a pen register order or a Title III warrant.<sup>13</sup> The legislation tasked the FCC with implementation and enforcement of CALEA.<sup>14</sup>

---

<sup>11</sup> Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in scattered sections of 18 U.S.C. §§ 229, 1001-1010, 1021).

<sup>12</sup> *Third Report and Order*, at para 2, CC Docket No. 97-213, 14 Rcd 16794 (1999); See also, Warren Pennington, *Communications Assistance for Law Enforcement Act Effectiveness in Dealing with Voice-Over-IP*, Capstone Project Proceedings Paper (2001), p. 1-2.

<sup>13</sup> *Third Report and Order*, supra n.12 at para 3.

<sup>14</sup> *Ibid.* at 3. The FCC has most recently released a Third Report and Order and an Order on Remand governing implementation. Communications Assistance for Law Enforcement Act, *Third Report and Order*, supra n.12; Communications Assistance for Law Enforcement Act, *Order on Remand*, CC Docket No. 97-213, FCC 02-108, April 5, 2002.

Although ISPs are not regulated by the FCC and further, the FCC has specifically found that CALEA does not apply to ISPs,<sup>15</sup> CALEA may apply in the case where an ISP connects to the PSTN (as in the case of a CLEC) or where common carriers are using VoIP transmission over their network. In regards to packet-mode technology, the FCC has found that CALEA compliance is required only when it is used to provide telecommunications service, not information services.<sup>16</sup>

Implementation of CALEA has been fraught with legal and technical issues, particularly with respect to VoIP and packet-based communications.<sup>17</sup> The FCC has granted numerous blanket extensions and extensions to individual carriers.<sup>18</sup> The FCC invited TIA (Telecommunications Industry Association) to “study CALEA solutions for packet-mode technology . . . that will better address privacy concerns.”<sup>19</sup> Subsequently, TIA put forth the TIA/EIA/J-STD-025 standard [J-STD] as an interim standard.<sup>20</sup>

Packet-based communications consist of packets of data that contain both call-identifying information and content information<sup>21</sup> carried in a stream containing packets from numerous individuals’ communications. The problem with CALEA compliance in a packet-based environment is three-fold: (1) call-identifying information that is beyond what an LEA is entitled to obtain cannot be effectively separated (2) the call-identifying information and the call content with a packet cannot be effectively separated and (3) target and non-target packets in the same stream cannot be effectively separated.

Although a packet may contain both call-identifying and call content information, a law enforcement authority (LEA) is only entitled to call-identifying information and not call content if operating under a pen-register order.<sup>22</sup> Although the FCC recognized call-identifying information as not limited to telephone numbers,<sup>23</sup> as was the case in the industry-developed J-STD,<sup>24</sup> it also recognized that not all dialing or signaling information identifies the origin, direction, destination, or termination of a

---

<sup>15</sup> Communications Assistance for Law Enforcement Act, *Second Report and Order*, Part III A, FCC 99-229, August 1999. See also, H. Rep. No. 103-827(I), at 21, (1994).

<sup>16</sup> *Third R&O*, supra n.12 at para. 48.

<sup>17</sup> See, Pennington, supra n.12. “It is with VoIP in mind that CALEA proves to be ineffective in light of its intended purposes when the legislation was enacted.” *Id.*, p. 1.

<sup>18</sup> See CALEA Section 107(c) Extension of Capability Requirements, Order, DA 01-2244 (Comm. Carr. Bur., Sept. 27, 2001); CALEA Section 107(c) Extension of Capability Requirements, Order, DA 01-1902 (Comm. Carr. Bur., Aug. 15, 2001); Public Notice, 15 FCC Rcd 22308 (Nov. 20, 2000); Public Notice, 16 FCC Rcd 4649 (Feb. 22, 2001); Public Notice, DA 01-1316 (May 31, 2001); and Public Notice, DA 01-1494 (June 22, 2001).

<sup>19</sup> *Third R&O*, supra n.12 at para 55.

<sup>20</sup> TIA/EIA/IS-J-STD-025A, “Lawfully Authorized Electronic Surveillance,” Includes Addenda 1 and 2, May 2000, Telecommunications Industry Association, revision of the original J-STD-025 published December 1997 jointly by TIA and Committee T1.

<sup>21</sup> The FCC found “call-identifying information” to be dialing or signaling information, not limited to telephone numbers, that identify the origin, destination, direction or termination of a communication. *Order on Remand*, supra n.13, para. 47-48. The FCC defined “origin” as a party initiating a call or a place from which a call is initiated; “destination” as a party or place to which a call is being made; “direction” as a party or place to which a call is re-directed or the party or place from which it came, either incoming or outgoing; and “termination” as a party or place at the end of a communication path. *Id.*, para. 48.

<sup>22</sup> A Title III warrant would entitle the LEA to both call-identifying and call content information. *Order on Remand*, supra n.13, para. 28-30.

<sup>24</sup> TIA/EIA/IS-J-STD-025, Lawfully Authorized Electronic Surveillance, Telecommunications Industry Association (1997) published jointly by TIA and Committee T1.

communication (the legislative description of call-identifying information), such as a social security number or an account number.<sup>25</sup> Thus, there is still call-identifying information to which an LEA may not be entitled, although the FCC found call-identifying information to encompass a broader range than the original J-STD.

Furthermore, when a communications provider captures packet communications for an LEA, it captures all packets in a stream, including non-target communications. Thus, not only is the privacy of the target and those with whom the target communicates impinged upon, but the privacy of other random people whose communications lie within that packet stream is also compromised. This is so because communications providers currently do not possess the technology to selectively separate these packets effectively.

There is debate that some commercial products are available to bring communications providers into compliance with CALEA with respect to packet data or VoIP communications, but there is strong contention that current solutions are ineffectual.<sup>26</sup> Critics maintain that these solutions have technical shortcomings resulting in some required information not being captured and/or that the information captured is overbroad.<sup>27</sup> LEAs maintain that Carnivore can effectively perform the needed separation function, but communications providers find implementation and maintenance of this solution so problematic that it is infeasible.

## 5.2. Role Based Identity and the Law

RBA does not conflict with CALEA compliance and may also be able to address some of these problems, particularly where information captured and delivered may be overbroad and infringe on privacy rights. In using an RBA model, a federation may employ authorization/authentication processes using only role-based information, not information specifying an identity. This will alleviate privacy and technical concerns for communications providers and users in several ways.

First, RBA does not conflict with CALEA since communications providers are required to produce information only to the extent that the information is present. Additionally, even if identifying information is not present in a packet for authorization/authentication purposes, the proxy/AS maintains that information and so it could be obtained if absolutely required.

Second, call-identifying information that surpasses what an LEA is lawfully authorized to receive, such as a social security number or an account number, would not be included in the communication if the federation chose not to use identifying information as part of an authorization/authentication process.<sup>28</sup> Thus, RBA relieves the communications provider from the unsolved problem of separating authorized call-identifying information from unauthorized call-identifying information.

---

<sup>25</sup> *Order on Remand*, supra n.13, para. 37.

<sup>26</sup> See, Jasomi Networks' New CALEA Technology Fixes Achilles Heel' of VoIP Legal Intercept Solutions, [http://www.jasomi.com/pr\\_calea.html](http://www.jasomi.com/pr_calea.html), visited July 29, 2003. See also, VeriSign Launches NetDiscovery Service for VoIP Interception at SUPERCOMM, [http://www.verisign.com/corporate/news/2003/pr\\_20030604.html](http://www.verisign.com/corporate/news/2003/pr_20030604.html), visited July 29, 2003.

<sup>27</sup> See, CALEA and Cable/ Part Two, MultichannelNews, April 24, 2003, [http://www.hostingtech.com/news/2003/4/24/Print/St\\_Nitf\\_CALEA\\_and\\_Cable\\_Part\\_Two](http://www.hostingtech.com/news/2003/4/24/Print/St_Nitf_CALEA_and_Cable_Part_Two), visited July 29, 2003.

<sup>28</sup> Note, an individual may still provide this information within the call content and an LEA may gain access to it with the proper scope of authorization, such as a Title III warrant.

Third, in a packet-based environment, there is technical difficulty in separating call-identifying information from call content since both are often contained in the same packet(s). However, an LEA may only be entitled to call-identifying information, not call content. The FCC has ‘resolved’ this problem with CALEA by leaving it to the courts. It found that although communications providers must have the capability of providing call-identifying information and that call content may not be able to be separated and excluded, it would be left to the LEA to obtain the proper authority to secure what information the communications provider could provide.<sup>29</sup> Alternatively, where an LEA only has authorization to obtain call-identifying information, but the communications provider does not have the ability to separate and exclude the call content, the FCC has left it to the courts to properly decide what the remedy may be.

In this case, where an LEA is not entitled to call content (as in the case of a pen register), RBA would eliminate identifying information that may have been included in the call content, since role-based information, not identifying information, would be asserted and included in the communication for authentication purposes.<sup>30</sup> Thus, although an LEA may still receive call content, an individual’s identity would still be preserved where they chose not to assert any identifying information as part of the authentication/authorization process.

Lastly, the privacy of others (non-targets and those not communicating to a target) may be preserved by applying RBA. Here, although packets of non-targets will be captured because they lie within the same stream as the target’s communications, no identifying information of non-targets would be present since role-based information would be asserted in place for purposes of authorization/authentication. Thus, privacy of non-targets is preserved by RBA in a federated environment that does not use identity information.

## 6. Conclusions

In this paper, we first examined two rather contentious terms, privacy and anonymity. We then provided a survey of some relevant technical background material. MORE We then briefly described the RBA models under development, as well as the motivation and rationale of these models. This included a consideration of the policy implications of RBA models, particularly as it relates to US federal law and policy. We ended by considering the how privacy, anonymity and law might co-exist.

In this paper, we demonstrated how proposed RBA systems might walk the line between privacy advocates by providing a means of anonymity, while allowing some accountability.

## 7. References

[AP] Associated Press, Verizon Must Reveal Song Swappers, <http://www.wired.com/news/digiwood/0,1412,58620,00.html> 2003

---

<sup>29</sup> *Third R&O*, supra n.12 at para 89.

<sup>30</sup> Note, again this does not eliminate the problem of the user conveying identifying information outside the authentication function, within the body of his communication or “call content.”

[Berthelsen] Christian Berthelsen, Assembly Lawmakers mad at response to killing privacy bill, <http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2003/06/19/MN127207.DTL>, San Francisco Chronicle 2003

[Ferraiolo] Ferraiolo D., Kuhn R., "Role-Based Access Controls", Proceedings of the 15th National Computer Security Conference, Baltimore MD, October 1992.

[Giacomoni] Giacomoni, J and Sicker, D.C., "A Cultural Neutral Identity and Privacy Evaluation Framework", unpublished, 2002.

[Goldberg] Ian Goldberg. A Pseudonymous Communications Infrastructure for the Internet, PhD Thesis, University of California at Berkeley 2001

[Liberty] see <http://www.projectliberty.org/>

[Mishra] Mishra P., et al., "Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML)", OASIS, May 2002. <http://www.oasis-open.org/committees/security/>

[NIST] "Role Based Access Control", National Institute of Standards and Technology. <http://csrc.nist.gov/rbac/>

[Oram] Andy Oram, CAN ANONYMITY MAKE US FREE?, <http://www.praxagora.com/andy/ar/anonymity.html> 1997

[Peterson03a] Peterson J., Polk J., Sicker D., "Role-based Authorization Requirements for the Session Initiation Protocol", SIPPING-WG Internet Draft, <http://www.ietf.org/internet-drafts/draft-peterson-sipping-role-authz-00.txt> (work in progress) March 2003.

[Peterson03b] Peterson, J., " SIP Authenticated Identity Body (AIB) Format" draft-ietf-sip-authid-body-01 (work in progress), February 2003.

[Pfitzmann] Andreas Pfitzmann, Anonymity, Unodservablility, and Pseudonymity – A Proposal for Terminology, 2001

[Rao] Josyula Rao, Pankaj Rohatgim, Can Pseudonymity Really Guarantee Privacy?, Proceedings of the 9<sup>th</sup> USENIX Security Symposium 2000

[Rosenberg] Rosenberg J., Schulzrinne H., Camarillo G., Johnston A., Peterson J., Sparks R., Handley M., Schooler E, "SIP: Session Initiation Protocol", Internet RFC 3261, <http://www.ietf.org/rfc/rfc3261.txt>

[SAML] SAML 1.0 Specification Set (31 May 2002): Committee Specifications (OASIS Standard as of 5-Nov-2002) <http://www.oasis-open.org/committees/security/>.

[Serjantov] Andrei Serjantov and George Danezis, Towards an information theoretic metric for anonymity, 2<sup>nd</sup> Workshop on Privacy Enhancing Technologies, 2002

[Shib] Shibboleth Architecture Draft, <http://shibboleth.internet2.edu/docs/draft-internet2-shibboleth-arch-v05.pdf>

[Sicker03a] Sicker, D., Kulkarni, A., Chavali, A., Fajandar, M., “A Federated Model for Secure Web-Based Videoconferencing”, IEEE Computer Society Press Proceedings of the International Conference on Information Technology: Coding and Computing, 2003.

[Sicker03b] Sicker D., Chavali A., Kulkarni A., Fajandar M., “SIP Bindings and Profiles for SAML”, Work in progress.