

Rochester Institute of Technology

RIT Digital Institutional Repository

Theses

2011

IP address registration database: Definitions for access, security, and implementation

Lesa Ouellette

Follow this and additional works at: <https://repository.rit.edu/theses>

Recommended Citation

Ouellette, Lesa, "IP address registration database: Definitions for access, security, and implementation" (2011). Thesis. Rochester Institute of Technology. Accessed from

This Thesis is brought to you for free and open access by the RIT Libraries. For more information, please contact repository@rit.edu.

Rochester Institute of Technology
College of Applied Science and Technology

IP Address Registration Database

Definitions for Access, Security, and Implementation

Lesa Ouellette

1/22/11

Thesis submitted in partial fulfillment of the requirements for the Master's of Science

Telecommunications Engineering Technology degree

Approval

Date:

Thesis Approved by:

Professor Ronald Fulle

Dr. Warren Koontz

Acknowledgements

I would like to express my deepest gratitude to the various individuals who supported my various learning and life endeavors for these many years: My husband who has provided unwavering support and a solid, safe foundation for all of my life's challenges and goals; Dr. Carolyn Slocombe, who has become a life coach and mentor, as well as a good friend, and supported this specific learning endeavor with her vast expertise, experience and guidance; The many learned educators at RIT who not only provided instruction but coaching, support and direction throughout this educational experience; My children, who provided me with a focal point to what really matters in life and the unique ability to offer a perspective on reality that only young adult men can offer; and my family who tolerated my inability to be present at so many events due to work and school schedules and loved me regardless.

With sincerest respect and thanks,

Lesa F. Ouellette

Abstract

This thesis analyzes the process of IP assignment and internet policing and proves that a national IP address database will allow law enforcement and governmental agencies improvements in real-time, secure access to subscriber identifying information without compromising the security and privacy of internet users. For the last three decades, the process of monitoring access, usage and IP address assignments has fallen on the internet service providers who allow access to the internet through their IP portals. Since they held the door to the internet, there was reasonability in the idea that they should monitor who goes in and out of that door. That concept remained stagnant because an alternative methodology did not exist and numerous regulations, fees, restrictions, and uses were developed over time to fit that model. This thesis details how the implementation of a centralized IP address database will provide a transition from the legacy 'provider assigned and monitored' model and offer a first-of-its-kind system that migrates policing functions back under the control of the policing authorities. The system establishes the best segregation of expertise, allowing the providers to provide service, the policing authorities to provide policing, and the governmental authorities, who define security safeguards, to also maintain it. Research methodologies incorporated in the development of this new concept include extensive interviews with law enforcement as well as in-depth research on internet legislative reforms, governmental systems, and security concerns and requirements. This review led to a system that successfully meets the needs of the user, the service provider, law enforcement, and governmental entities alike.

Table of Contents

Approval	i
Acknowledgements	ii
Abstractiii
Table of Contentsiv
List of Figures	vi
Introduction	1
A Review of IP Address Management Today	4
IP Address Registration Database	9
Public Confidentiality and Privacy	13
ISP Support	16
Law Enforcement and Government Agencies	19
Legislative Reforms	28
Migration to IPv6	39
Wireless Migration to 4G	42

The Implementation	47
IPAR Record Format	54
Query & Selection Application	58
Requestor Accounts	65
Who Pays?	74
Future Development and Expansion	80
Conclusion	82
Addendum A – <i>Cox Communication rate sheet for subpoena processing</i>	83
Addendum B - <i>2009 Comcast Customer Privacy Notice</i>	84
References	93

List of Figures

Figure 1: IANA	4
Figure 2: DMV Geographic Agencies	53
Figure 3: IPAR Data	58
Figure 4: IPAR Login Screen	59
Figure 5: IPAR Name Query Screen	60
Figure 6: IPAR Address Query Screen	61
Figure 7: IPAR Address Report	62
Figure 8: IPAR Registrant Login Screen	63
Figure 9: IPAR Manual Data Entry Screen	64
Figure 10: IPAR Error Messaging Example	65
Figure 11: IPAR Requester Account Application	69
Figure 12: IPAR Authorization Form	70
Figure 13: IPAR Provider Submission Account Registration Application Page 1	71
Figure 14: IPAR Provider Submission Account Registration Application Page 2	72

Introduction

When IPv4 was first outlined in RFC 791 in 1981 it was the fourth version of internet protocol and the first to be introduced for public use. In its introduction its scope was defined as follows: *“The internet protocol is specifically limited in scope to provide the functions necessary to deliver a package of bits (an internet datagram) from a source to a destination over an interconnected system of networks..”*¹ In 1981, there was no realization as to what an ‘interconnected system of networks’ was to become over the next 30 years. A globally interconnected communication, financial, social, economic network, where everything from video games to telephone service and vehicle navigation was intertwined in a single network, was unforeseen. An address structure that could provide 4,294,967,296 unique addresses seemed able to accommodate interconnectivity for all perpetuity. Teleport into the future 30 years and we find a world where much of our existence, from our work to our home to our government, could not function without a world-wide network that is always on and always available. Presently most technology providers are now working on a migration to the newest version of internet protocol, IPv6, to accommodate the exponential growth in networked applications and interconnected users. This new version of IP, based on a format of 128 bits, extends IP addressing to 3.4×10^{38} unique IP addresses. As our predecessors believed with IPv4, technologists once again believe this new quantity should accommodate all IP addresses needed for perpetuity. Will it? It sounds limitless until one begins to count the number of

¹ Information Sciences Institute, University of Southern California. *Internet Protocol. Darpa Internet Program Protocol Specification.* <http://www.ietf.org/rfc/rfc791.txt> (accessed January 2011).

devices that can at some point become 'enabled' and suddenly the number seems only reasonable and not limitless.

We look at our IP processes and our evolution of networking through the same 1981 eyes.

Many functions or processes are directed toward a network environment based on a single point in time and then work to keep their place intact as the technologies around them change.

This is commonplace when looking at the historical legislation that has attempted to modify or direct the internet and its use. With a legislative process mired in partisanship and lobbying, legislative orders can take years to implement. Often by the time they are implemented the technologies they are based upon have changed. Dictates are implemented based on a point in time without proper preparation of what is to come. This holds true to the very components of the internet itself and the most basic connecting block to that global interface which is the IP address. The national model of IP address assignment, as well as its subsequent use, storage, protection, and investigation, are all based on models that were developed back when IPv4 was going to automate the business world and long before IPv6 meant we might have enough IP address space to automate every single tool in our lives. In 1981, without the vision to see where this new internet could go and the comprehension that this new internetworking platform could one day become a new criminal front, the processes for protection of a user's internet security were undefined as were the methods to protect and police it. Without the knowledge or tools to perform these monitoring and policing functions, the tasks fell upon the one group that could, the service providers who were providing the IP address token that opened up the global internet for use. Service providers moved from the role of providing internet services to their subscribers, to a role of providing internet monitoring, logging and

reporting to the government and law enforcement. While subscribers were willing to pay for the use of the provider's network, governmental agencies were not willing to pay for the usage surveillance they required of those same subscribers, leaving the cost burdens to fall upon the provider and ultimately back on the subscribers themselves. The process formed as a reaction to changes that government and law enforcement were not prepared to address. A world wide educational and business integration platform was suddenly an open access portal for unrestricted and anonymous criminal activity. Stepping back and now assessing the reality that is the internet, and the freedoms that US citizens have grown to expect in every aspect of their lives, the process of providers being the entity of internet surveillance seems archaic and dysfunctional. There must be a better way to bring the policing function to the agencies that are appropriately trained to perform it.

This thesis analyzes the process of IP assignment and internet policing and proves that a national IP address database will allow law enforcement and governmental agencies improvements in real-time, secure access to subscriber identifying information not accessible in today's traditional provider-only process, without compromising the security and privacy of internet users.

A Review of IP Address Management Today

Most internet users are unaware of the systems or processes that support their access to the internet. Very simply they want the internet to be available 24x7x365 and, other than the monthly fee to their provider, know very little about the technologies that get them there. Here is a recap of how the internet IP process works.

Internet service providers (ISPs) purchase ranges of IP addresses from an Internet Assigned Number Authority (IANA). This IANA provides the ISP with exclusive ownership/use for the IP address space for as long as the ISP continues renewal. ISPs then divide these IP address ranges into smaller allocation blocks, typically segregated by geographic regions. Within these allocation blocks individual IP addresses are then leased to the ISP's customers for a monthly subscription fee. *Figure 1* shows the chain of IP address allocation for providers within the United States.

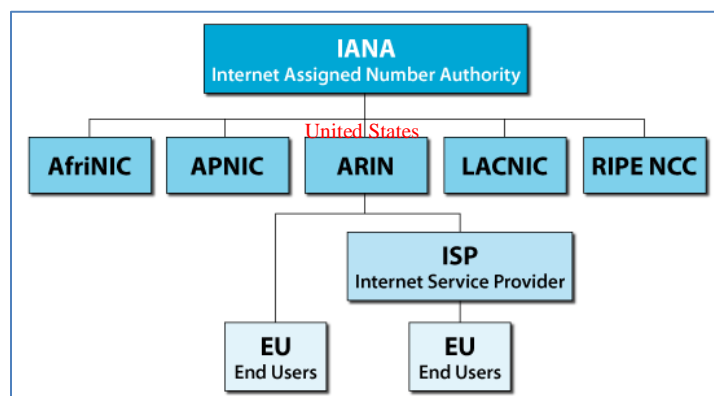


Figure 1: IANA

This subscribed IP address provides the customer with a connection method or access point to the Internet. In order to adequately share the IP address resources across the ISP's customer base, customers share a dynamic pool of addresses. Upon subscribing, an IP lease is assigned to the customer and is given a varying lifespan for the customer dependent upon customer use. While a standard lease period may range from one day to several months, customer usage often regulates how often a subscriber's IP address will change or how long a customer may retain one unique IP address. The process works as follows:

A customer purchases data services from an ISP and receives an IP address upon connecting through the provider's network. The service provider issues the customer a default lease of <14 days> for the IP assignment (a typical value). If the customer does not regularly use the IP address (not using their computer regularly or powering down their data modem for extended periods of time) the IP address will be pulled back into the allocation pool to be assigned to another subscriber for internet use. Should the first customer resume internet connectivity, the ISP would assign the customer another IP address from the pool. This scenario outlines the process of 'dynamic' IP address allocation, allowing a range of IP addresses to be shared across all of the provider's subscribers. Without this dynamic process, IP addresses would become static, and once assigned would remain with a customer for perpetuity. Static assignments would greatly diminish the number of IP addresses available for new subscribers, having tied up assignments for subscribers who may no longer be using them or use them infrequently.

This assigned IP address is the Internet access point for the subscriber. ISPs are able to link the IP assignment to the customer in order to track allocation of bandwidth and service usage. This IP address links the customer to their internet activity and is the technical connection to ensure activities on the World Wide Web accurately make their way through the ISP back to the intended computer / user. This ability to link the customer to their specific activity on the internet is a technical requirement. It is also the basis for broad concern about the privacy of a subscriber's internet activity and identification relative to cyber crime.

While desiring always-on connectivity, consumers have grown more cognizant of security liabilities inherent in the internet. Identity theft and cyber crimes have become frequent topics for local and national news making it important to understand that today's IP management process was developed for a reason. Instances of internet crimes increased at staggering rates, with criminals operating in complete anonymity in an environment nearly free of policing. After 9/11, few citizens would argue that national security is not vitally important and none would be tolerant of a government that allowed another terrorist act upon its citizens. The argument for accurate and timely internet identification information is valid when it relates to criminal or terrorist activity. How can that criminal activity be separated from the millions of legitimate internet transactions that occur every day?

For law enforcement officials, the process of locating a cyber criminal can be arduous and unfruitful. Because ISP were not historically required to retain subscriber IP address data, many didn't or routinely only kept data for 30 days or less. When investigators identified criminal

internet activity, they were unable to determine who it originated from because ISPs either didn't have it, or the process to request it took so long that data was long since purged by the time it was requested. There was no legal leverage requiring the ISPs to track the data or keep it. On the other side of the issue, ISPs also had a legitimate requirement to protect the privacy of their subscribers. Unauthorized access to subscriber information, by linking internet usage to the IP address assigned to the customer, could result in hefty penalties to ISPs. The middle ground came in the creation of the two-subpoena process where law enforcement and government agencies could legally subpoena the ISP to provide subscriber records. The process is as follows:

Investigators identify a screen name as the originator of a criminal activity. The law enforcement unit must subpoena the provider of the screen name (say AOL) to obtain the IP address that the screen name is being accessed from. The legal process of providing the subpoena to AOL and the subsequent processing time of the subpoena by AOL can take many days or weeks. Here, the AOL email/instant message service is an application operating on top of the internet connection provided by the ISP.

When the investigator receives the response to the subpoena from <AOL> they next have to research the IP address provided to determine which ISP owns that IP range. The IP addressed could be owned by Verizon, Comcast, or any one of hundreds of small ISP providers around the country. When the determination is made as to who's network the activity is occurring on, law enforcement must then provide a second subpoena to the ISP requesting subscriber name and

address information. As was the case with the first subpoena, a response can take anywhere from several days to many weeks. The response time, from an investigators perspective, is too long to be productive or reasonable. They can identify criminal activity but have no ability to locate the whereabouts or identify of the criminal long after the activity has occurred.

Keep in mind that the process outlined here is the best-case scenario. Where the subpoena process is a legal matter, any error... typographical or otherwise... can result in the document being returned for correction. Any such error only adds to the delay in obtaining information. Many law enforcement agencies recount having to wait a year or more for information to be provided. These delays only increase the likelihood that data will no longer be available, no longer in archive at the ISP. Nearly half of subpoenaed information for ISP data is returned as 'no data on file'².

For the ISP it is also a matter of quantity. In an email interview with one ISP's Senior Director of Compliance and Legal Affairs, the compliance team can receive anywhere from 350 to 450 subpoenas per month. When those subpoenas are broken down to the individual IP addresses to be researched, the number grows to more than 630 subpoenaed IP address requests per month. The team of five subpoena processors is responsible for documenting, researching, processing and responding to each of these subpoena requests. While the average response is 10 days, many can take much longer depending upon the date of the original activity and whether the data has been archived offsite. As high as this volume may seem, this quantity

² Zonk. "US Government Demands Data Retention." (June 2, 2008), Slashdot. (accessed October 19, 2010).

only reflects requests specific to IP address information (only data service activity) and is not inclusive of IP phone records which are handled by a third party. Inclusion of VoIP records would double the volume of responses this ISP is required to handle each month. Once subpoenaed, data relative to the subpoena must be retained for a period of 3 years, compounding data storage and privacy liabilities.

This requirement for ISPs to retain IP information about their subscribers has led to numerous legislative and systematic changes both for the provider and the consumer. There is a legitimate need to link consumers to their internet activity. There is also legitimate concern that in doing so, private information about a consumer can be accessed. Could there be a better way to allow law enforcement quick access to identify criminal activity while better safeguarding the privacy of customer identifiable information?

IP Address Registration Database

Conceptual Definition

Let's compare an IP address to a vehicle's license plate. While a license plate, by itself, does not provide the public with any details of the user / owner of the vehicle, a license plate does provide information when it is retrieved from a secure database managed and accessed by State and law enforcement agencies. The vehicle registration database does not contain a log of every highway, road or bridge a driver uses, or the speed at which they drove, or the time of

day. Instead, the database contains a mechanism to link a license plate to an owner's personal information specific to the vehicle being queried. Any determination of infraction or restriction is up to law enforcement to identify and record. The nation's highways remain available for open use with the exception of having to pay for service on freeways and toll roads. At the simplest level, the only information that can be determined by the license plate itself is the state of registration and the month and year of registration.

Now let's apply this to an IP address. The IP address, by itself, does not contain or provide any personal information of its owner / user. While the owning ISP can be identified, similar to the state of registration of a vehicle tag, personal information about a specific user is not available strictly by view of the IP address. As each user is assigned an IP address, often after paying a toll to an ISP for use of that internet highway, that user has open and unrestricted access to all lanes on the internet. While the ISPs provide the opening through the toll to use the roads, they do not provide monitoring services to determine who is exercising lawful or unlawful behavior. That policing function is performed by governmental or law enforcement agencies using various tools within their arsenal. In the same way a patrolman identifies offending vehicles and targets them for further identification, the same is true of users on the internet and their assigned IP address. Until such time as their activity triggers further inquiry, the user is unhindered from using the internet and all its capabilities.

To implement this theory of a centralized IP address database, there must be both an input of information from the service provider and storage, indexing, and archiving data systems at the state and/or federal levels. Here is how it works:

Customer X purchases internet service from an ISP such as Comcast. Comcast assigns the customer an IP address of 77.10.176.18. That transaction is sent to the IP Address Repository (IPAR). The data string contains such information as the IP address, date and time of assignment, Customer X, and an ID tag associated with the ISP. While a typical IP reservation period is 14 days, with continued use and limited system maintenance the user can maintain an IP address for extended periods of time, sometimes up to a year or more. In the event a new IP address is issued, regardless of when or by what mechanism, that IP record is sent to the IPAR as an update record. The update record contains Customer X, IP Address assignment, date & time, and ISP id tag. Over the course of use, the IPAR will be updated multiple times per internet subscriber. Customer X will show multiple entries, each with an IP address and date and time of assignment. IP Address information can be sorted to identify all IP assignments to named users, to physical location or other groupings.

Here are several of the concepts in play in a state and federal IPAR system:

- a. Historical recording and archiving of IP address information is moved from the ISPs to state, federal and/or law enforcement agencies.
- b. Security management of IP information would be maintained by the same entities already responsible for managing highly confidential information. Similar to the vehicle registration database, these entities already keep confidential information such as:
 - a. vehicle registrations, restrictions, and fines

- b. social security information including social security numbers, benefits and litigation
- c. taxation information including compensation, employment and garnishments
- d. criminal records by jurisdiction area

These are entities already well versed in the management and retention of very confidential information...information that is much more highly confidential than an IP address.

- c. Access to customer identifying information becomes immediate. The common, two-subpoena process is reduced by one, if not both subpoena processes.
- d. Law enforcement would continue to be held to requirements of reasonable cause for information requests.
- e. Small providers, who could not afford the cost of data collection and retention, can support an IPAR implementation, increasing availability to subscriber information that was otherwise unavailable.
- f. There is no change in the existing definition for the line between reasonable search and concerns relative to accessing the IPAR for surveillance. The same statutory and legislative proceedings exist, with the only change being the caretaker of the information.

- g. Yahoo, MSN, and Google fall under separate and specific definitions for Internet ‘applications’. Consumers already have access to the highway before they can access these applications. These applications would continue to be subpoenaed for search or usage information, in the same way a Transit Authority can be subpoenaed for records on toll interchange usage.

Public Confidentiality and Privacy

There lies a dichotomy in concern relative to the internet. Users want the unhindered freedom to use the global internet at their own discretion. Users also want, ideally expect, to be safeguarded from attack, exploitation, surveillance and other invasions of privacy while exercising their internet freedoms. With the internet being a somewhat lawless environment, service providers bear increasing burdens to ensure the safety of subscriber identity and activity. Limited monitoring and policing, however, has allowed the internet to grow as a safe haven for criminal activity. How, then, does the IP Address Repository provide improvements to securing confidential information and protecting the privacy of consumers?

The IPAR would follow similar requirements as defined in the Driver’s Privacy Protection Act or DPPA. The DPPA was implemented in 1994 to ensure the protection of personal information contained within the records of the Department of Motor Vehicle.³ This Act outlined specifics for restricting the use of a license plate or vehicle identification number (VIN) from being used

³ Epic.org. “The Drivers Privacy Protection Act (DDPA) and the Privacy of Your State Motor Vehicle Record.” *Electronic Privacy Information Center*. <http://epic.org/privacy/drivers/> (accessed October 11, 2010).

to search for the name of the vehicle owner. In addition, this Act defined specifics for DPPA permissible use, outlining processes for obtaining access to records that contain personal information. Law enforcement would be allowed protected 'search accounts' to have frequent, ad hoc access to information. Other entities, unless granted specific approved access, would have no accessibility to the private information.

The IPAR would have very similar guidelines and restrictions. Unless an entity is granted specific 'permissible use' access to personally-identifiable information, the database remains restricted from access. While legislation such as the Patriot Act⁴ lessened governmental restrictions on internet surveillance, law enforcement agencies are still required to obtain a court order before they are authorized to monitor internet activity. This means that law enforcement and governmental agencies would not only have to apply for access to the IPAR's information, they would also have to request and obtain a court order before they could use the information from the IPAR for internet activity surveillance.

Supporting an IPAR means ISPs around the country must provide up-to-date information feeds to the central IPAR. Issues concerning the security of these transactions must be identified and addressed. On the receiving end is an agency used to receiving and protecting very confidential information. Take, for example, the Internal Revenue Service and electronic tax filings. In 2009, more than 95 million people filed their income tax returns electronically.⁵ These are

⁴ Lithwick, Dahlia and Julia Turner. "A Guide to the Patriot Act, Part 1, Should you be Scared of the Patriot Act?" <http://www.slate.com/id/2087984/> (accessed October 1, 2010).

⁵ KOLD, News 13®. "IRS E-File, Free File and other electronic options", IRS.gov. <http://www.kold.com/Global/story.asp?S=1072219> (accessed October 1, 2010).

electronic transactions that contain an individual's social security number, date of birth, address, annual income, and much more. To protect the confidentiality of the information contained in these transactions, secure channels must be configured to ensure the safest delivery of this information. As outlined by the IRS website⁶, safeguards include:

- The IRS *e-file* System is not done over e-mail
- The IRS *e-file* System has many built-in security features
- The IRS *e-file* System employs multiple firewalls
- The IRS *e-file* System uses state of the art virus and worm detection
- The IRS *e-file* System meets or exceeds all government security standards
- The IRS *e-file* System is constantly tested for weaknesses by penetration testing
- All Internet transmissions will use SSL (Secure Sockets Layer) encrypted security measures.

If these methods provide secure channels for the delivery of extremely confidential tax information, these same methods can be deployed to ensure IP address transactions to the IPAR are also delivered safely. ISPs who feed IP data to the IPAR would be required to transmit only packets that are encrypted. On the receiving end, the IPAR would be positioned behind multiple firewalls that would only allow registered providers through.

Keep in mind that data being fed to the IPAR contains far less confidential information than an electronic tax filing. The IPAR transaction contains only an IP address, along with the name and address of the owning subscriber, and a tag to identify the submitting ISP. In a two-part authentication scheme, this transaction would house only one part of the information needed to discern internet usage. Usage records would still be legally protected within the ISP and/or within internet application hosts such as Google, AOL, and Craigslist. Those entities would still

⁶ IRS.gov. "IRS e-file: Secure Online Tax Filing". <http://www.irs.gov/efile/article/0,,id=121477,00.html> (accessed October 2, 2010).

own the protection responsibility of the usage records of their subscribers and require court orders in order to release the information.

ISP Support

An IPAR solution offers several advantages to service providers. Growing data retention requirements mean ISPs have progressively taken on increasing burdens in keeping more and more data relative to their subscribers and subscriber activity. Increasing data requirements means increasing back-end systems that support both the storage of the data and the indexing mechanisms to retrieve it. The more data stored, and the more data written to tape and offsite storage, the greater the liability and risk of security breach. In addition, subscriber information maintained by the ISP contains much more than the IP address. This data contains all subscriber activity from usage, to payment transactions, to services including email and wireless accounts.

Having the only systems that marry activity to IP address means ISPs face increasing pressures to become the monitoring and policing authority for the subscribers they service. Recent legislation implemented in the United Kingdom, known as the Digital Economy Bill, allows authorities to not only require ISPs to monitor their subscribers' activities, but also hinder access for users identified as engaging in criminal activity on the internet⁷. With similar

⁷ Parr, Ben. "UK Passes Controversial Digital Economy Bill". <http://mashable.com/2010/04/07/digital-economy-bill/> (accessed October 3, 2010).

legislation considerations in the United States, ISPs face ever increasing policing requirements.

An IPAR implementation helps in the delineation between provider and policing functions.

To support an IPAR implementation, providers must provide immediate data feeds to the central IP address database. Each time a DHCP system provides an updated IP address to a customer, the ISP must send a copy of that IP assignment, along with the name and address it is assigned to, to the IPAR. With this method, law enforcement and government agencies no longer need to rely on the ISP to provide IP information when policing authorities request it. Instead, the burden of policing activity can be left in the hands of law enforcement that are then enabled with immediate access to IP information as it is needed. Responsibility for the policing of the internet is a definition both law enforcement and service providers agreed needed to be defined and the IPAR helps with that designation.

In addition to the reduction of policing requirements for an ISP, an IPAR also helps by significantly reducing the labor and systems needed for IP address and subpoena management. The subpoena process, by itself, requires application and systems to create, index, and store the plethora of subpoena requests received by the services providers. Legal respondents must track incoming subpoenas, recording the information provided in response, and tracking the processing time in order to meet legal requirements. With an IPAR providing a reduction in subpoena requests to the ISPs, there is a corresponding expense reduction realized by the ISP which can reduce such costs from being passed on to the consumer.

Not all burdens are removed from an ISP however. While subpoena processing is expected to decrease, new data-delivery systems will have to be implemented to provide transaction data to the IPAR database. These systems would have to support real-time transmission of dynamically or statically assigned IP addresses, provide SSL encryption of the transmitted data, and support authentication mechanisms with the IPAR. These systems would have to comply with 24x7x365 operations and have support staff to maintain and support them.

For data delivery to work properly, ISPs will be required to register with the IPAR to obtain an ISP identification tag, or ISPID (eye-spide). This ISPID will be appended to IP address records in order to identify the service provider that is providing the data. National providers that service customers in multiple areas of the United States, such as Comcast, will be required to obtain an ISPID for each jurisdictional area, typically defined as a major metropolitan area (such as Boston or Los Angeles) or state (New Hampshire). Along with an ISPID, registration to the IPAR provides the ISP with a secure tunnel to be used to submit data. This secure tunnel is provided as a uniquely assigned IP address that is allowed through the receiving firewalls. For incoming transactions, this incoming network IP address is matched to the ISPID on the record as a method to twice authenticate the provider and accept the record.

Non compliance with the IPAR registration would follow similar punitive actions and fines as is true for non-compliance with data retention requirements. While ISPs could be assessed a registration fee to obtain an ISPID, greater cost emphasis would be placed on non-compliance penalties to encourage proper use of the IPAR.

Law Enforcement and Government Agencies

In an interview with Detective Sergeant Lang of the Maine State Police Computer Crimes Unit⁸, I asked what it was that law enforcement really needed from an ISP. He listed these items:

- Easier access to information. Of particular interest is access to name and service address for IP address holders. While service address is critical in identifying the location of the activity, some ISPs provide billing addresses which do not always correspond to location information for the customer.
- Real-time information. Sergeant Lang cited a recent incident where a suicide threat was uncovered on a website posting. These are situations where the information must be expedient and accurate to the hour. He also cited other cases of death threats where similar access to emergency information was needed.
- Historical information. In normal investigation of computer or internet crimes, there is often a pattern to the activity. Having the ability to identify a user, and then see the length of time they held the IP address, or where an address was before or after, helps in solidifying evidence. This is generally information that is not readily available to them in the current subpoena process. Subpoenas typically ask for the IP address for the specific event... a particular IP address at a particular date and time.

⁸ Lang, Glen. Phone interview with Sergeant Lang, Maine State Computer Crimes Unit. 6 October 2010.

- Access to information that has been otherwise unobtainable. Certain small providers have been unable to keep up with the technological growth required to meet the subpoena requests. These small companies “never provide a response”, according to Lang, leaving them no method to investigate criminal activity within those service areas. Another instance involved a large company that had recently filed bankruptcy. Bankruptcy rulings did not mandate the company comply with prior subpoena reporting requirements, thus all requests for information were being returned as ‘no records’.

What recourse is there for these entities that do not comply with internet service data requirements? The most common recourse for providers who do not maintain records is to require them to appear in court as the ‘custodians of record’. If the records are not provided electronically or physically, then the provider can be summoned to court to personally appear to testify to the data requested. If the records are not provided or maintained however, then an appearance serves little purpose other than to discomfort the ISP. A provider, with no records to substantiate the evidence, bears little credence in the hearings.

These requests from law enforcement remain consistent. They need improved and timelier access to information, easier methods to identify activity related to copyright infringement and child endangerment, and improved support for emergency situations. Without access to such information, law enforcement has no recourse but to require the providers to provide the missing information. Lines relative to policing responsibilities are grayed as a result. The IPAR

enables law enforcement the control to police activity and set more definitive boundaries on responsibilities for the policing functions, where law enforcement is the best trained to do so.

There is an additional benefit inherent in the IPAR relative to law enforcement. While cyber investigators need quick access to information, they must also continue to follow proper access methods to obtain it. This IPAR format provides continued support of the process for search and seizure of computer equipment. The 'internet' by itself cannot instigate a crime. It is nothing but an access highway and it is the users of this road that are using it appropriately or not. The goal for investigators is to narrow down the activity to a point where they can reasonably request a warrant for the retrieval of computer equipment. Access ultimately to the computer where the crimes occurred is key. The perpetrator's computer can, by itself, be deemed as contraband. By definition, contraband is *any property that it is illegal to produce or possess*⁹. When that computer contains child pornography which is illegal to own, the computer is now deemed contraband and meets the criteria as illegal to possess. The computer can also be the 'instrument' of a crime. If the computer was used in the creation of illegal pornography, or used to download copyrighted material, or used to hack into a database, it is now actual tool or 'weapon' used to commit a crime. In an online criminal investigation this is the true end target to conclude the investigation. Obtaining access to that final computer, however, falls under very specific guidelines for search and seizure.

When online activity is identified, law enforcement today has to subpoena the ISP to identify the owner of the IP address in question. In an IPAR concept, law enforcement can obtain that

⁹ Contraband. Legal definition of Contraband by the Free Online Dictionary. <http://legal-dictionary.thefreedictionary.com/contraband>. (accessed November 2, 2010).

information from the IPAR database removing the lengthy subpoena process. This IPAR data is important for other reasons far beyond expedited access. IPAR allows greater compliance acceptability and a more consistent format to the investigative data that will eventually be provided in the criminal proceedings. Depending upon the ISP and their system capabilities, respondent data can come in a variety of forms. Less sophisticated providers have fewer data reporting options and may be able to provide little supporting evidence other than their statement. Subpoena responses can vary significantly between providers. IPAR helps to eliminate inconsistencies as the data returned in a query is identical from one investigation to another.

Similar to records obtained from the Department of Motor Vehicles database, consistency in form and content is valuable in provided improved credibility to the records. Obtaining data from a secure, registered entity like the IPAR reduces the likelihood that IP address evidence would be inadmissible. It provides a method to standardize the evidence record going forward. This is important when criminal investigations reach the critical juncture of search and seizure. According to Sgt. Lang, the end computer can be the most critical piece of evidence tying together the records from the ISP and records from their investigation. The process to seize the equipment, however, can be more difficult than the original subpoena for information. The key difference is that seizure requires a warrant and warrants differ greatly from subpoenas. In the subpoena process agencies are asking to be provided information. In a warrant, agencies are asking for permission to go get it. It is the difference between 'please send it to me' and 'I'm coming to take it'. This makes the legal process of search and seizure more stringent and therefore the IPAR more helpful.

Obtaining a search warrant requires a judge or magistrate to provide a written order to search and obtain physical property or assets. These are only granted in criminal investigations and require investigators prove probable cause that there is substantiated evidence enough to approve the search. Proving probable cause requires submission of a formal affidavit along with the evidence gathered during the investigation. Evidence can vary from case to case even when the cases themselves are very similar. Submissions of report data from the IPAR allow a single format and consistent method to tie users to IP addresses when obtaining warrants. Any synergy can improve the success of determining probable cause. IPAR data is coming from a state secured entity, very similar to motor vehicle records submitted in criminal hearings, giving it the proper credence to validate the warrant request. In a fully functional IPAR implementation this extract can become the standard for IP address identity evidence.

Beyond the requirements of individual law enforcement requests are several federal requirements relative to law enforcement, lawful intercept of data, and CALEA compliance. CALEA, which stands for the Communications Assistance for Law Enforcement Act, is a law enacted in the United States in 1994 .. *“To amend title 18, United States Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for Law Enforcement purposes, and for other purposes.”*¹⁰ Often called the ‘wiretapping law’, CALEA brought about several important compliance rules relative to ISPs and accessibility to data. Keeping in mind that wiretapping in 1994 was primary comprised of tapping into copper lines and interception of traditional voice traffic, very quickly this requirement transitioned into interception of VoIP and data packets on mostly IP networks. Beyond the needs to produce

¹⁰ CALEA – Definition. wordIQ.com. <http://wordiq.com/definition/CALEA> (accessed November 3, 2010).

records in response to legal requests, CALEA brought about a new requirement for ISPs to enable interception of real time call or data exchanges.

While CALEA attempted to provide law enforcement with improved access to real-time call detail data, it was very slow to implement. Carriers networks in the mid-90's were fairly open to interception by their very architecture making carriers slow to accommodate structural changes relative to compliance on this new initiative. By 2004, the United States Department of Justice filed a petition to expedite compliance requirements of the carriers to give them a deadline to meet the requirements of the original law. At that time most carriers were transitioning to VoIP architectures bringing new sets of challenges for law enforcement relative to interception of data, and forcing heightened demands for compliance with the new law. In response, CALEA laws were updated in 2006 to mandate a compliance deadline of May 14, 2007 for carriers and ISPs.¹¹ This adopted "Second Report and Order" of 2006 also defined the responsibility of development and implementation costs as being solely on the carriers and ISPs. While the financial responsibilities were now defined as a cost for the providers, the new Order also went on to allow carriers the use of third parties providers to assist in meeting the deadline and reporting requirements. Most importantly, this new revision of CALEA defined broadband and VoIP providers as "telecommunication carriers" making the final designation that new broadband providers and traditional telephony carriers were now combined under the same classification relative to data intercept and collection.

¹¹ FCC 06-56. Federal Communication Commission. "Second Report and Order and Memorandum Opinion and Order", May 3, 2006. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-56A1.pdf (accessed November 7, 2010).

Compliance with this new CALEA requirement involved many technological changes to service providers. The concept of 'intercept' meant carriers had to provide a method for law enforcement to intercept subscriber's real-time communication. This was achieved by either installing intercept hardware that would allow agencies to tap into communication whenever needed, or installing forwarding devices that automatically transmitted intercepted data to law enforcement while simultaneously forwarding that traffic along to the intended party. Neither of these endeavors was easy or inexpensive. While ISPs complained about uncompensated costs, new third-party providers arose whose purpose was to manage CALEA compliance and intercept processes for the ISPs. Interception and legal compliance, both from a hardware and a reporting perspective, could now be outsourced.

The premise of intercept and outsourcing also plays a role with the implementation of the IPAR. Legal compliance for intercept had a deadline of May of 2007, which means a majority of providers now have some method to provide intercept data to law enforcement. This concept of intercept works hand in hand with IP data routing to the IPAR. The process of forwarding intercept data to law enforcement is very similar to the process of forwarding IP address assignments to the IPAR. The IPAR adds a unique verification point between the intercepted real-time communication and the confirmation of the identity of the subscribers that initiate that communication. Real-time data in the IPAR provides a legal method to substantiate the intercept data being forwarded to law enforcement. With the right systems in place, government agencies could integrate the data from the two systems into one comprehensive and inclusive record of data identity and activity.

New third-party providers that offer CALEA compliance services can also integrate well with the IPAR. Since the introduction of intercept in 2004, several providers of compliance services have emerged with some offering hardware intercept services and others providing a full sweep of legal compliance processes and services. One such provider, Neustar[®], touts the following: *“Our expert systems account for and track jurisdictional distinctions and nuances of all 50 states and all federal agencies and courts – uniformly applying them to each demand for customer records.”*¹² In addition they offer:

- A defined strategy and turn-key solution for end-to-end CALEA compliance for voice, VoIP and broadband internet service.
- A primary interface to the LEAs (law enforcement agencies) and prosecutors when a challenge to an order’s validity is required, or if a clarification of scope and reasonableness is necessary.

While Neustar is not unique in these offerings, of importance here are the specifics to broadband providers and the existing interface to law enforcement. For the ISP, if third parties such as Neustar now have the ability to intercept traffic, they also have the ability to integrate with the ISP for purposes of collecting and forwarding data to the IPAR. This is a critical offering for providers who can’t meet the requirements for providing data to the IPAR whether due to cost or technical challenges. Having to be compliant with intercept requirements means providers had to be ready for integration methods such as those offered by a company like Neustar. These services can be utilized for the ISP beyond the intercept requirement and

¹² Neustar.com. “When law enforcement calls, will you be ready?” <http://www.neustar.biz/services/legal-compliance-services/court-ordered-records-production> (accessed December 28, 2010).

provide an alternate method of getting data transferred to the IPAR. As stated above, Neustar also purports to understand the 'jurisdictional nuances' of all 50 states. This aligns well with the state-based format of the IPAR and dissecting the data into the proper jurisdictional units. For smaller ISPs, third party providers can be the key in completing integration with the IPAR.

Additionally, having functionality through third party vendors means companies like Neustar can offer an additional service. While Neustar is being used as the mediator for the intercept process with law enforcement, they can also extract IP address information, integrating the two processes into one. The benefits here are two fold. For the ISP, the IPAR process can be outsourced to a provider that has already met the authorization guidelines for collecting and processing sensitive legal information. Outsourcing could be more cost effective for the ISP, in particular if they are already using an outside source for intercept functionality. Beyond the ISP benefits, there could be a significant opportunity in having the two processes married within the same third party outsourcer. Having the existing functionality to intercept and collect real-time communication means providers like Neustar also have the ability to link that data to the IPAR, forming one complete record of activity and IP address assignment. While integrating this data isn't necessarily of interest to the provider themselves, it is critical information for the government agencies at the receiving end of the intercept data. These third parties could provide an interim database service, which sits between the IPAR and the intercept systems, providing a very unique and all-inclusive service for law enforcement.

Lastly, beyond the opportunity for data integration, most of these third parties additionally offer subpoena and legal compliance services. This could make them a possible one-stop-shop for ISPs as coverage for all law enforcement compliance initiatives. Services include:

- Court ordered records production
- Legal and / or customer notifications
- Records retention
- Legal process wording

While fulfilling the obligations of providing timely IP data to the IPAR, third party providers could complete the entire outside intercept and legal document processing functionality, offering a critical service of integrated data for law enforcement and reducing the burden on the ISPs.

Legislative Reforms

While law enforcement embraced rules such as CALEA, privacy advocates complained about the open ability for the government to tap-at-will. Adding the growing concerns of internet security, legislatures have worked for more than a decade, to define rules to regulate the use and activity of the open and unrestricted internet. Without having any control on the physical or network layers that comprise the internet, law makers were left with limited alternatives other than to require service and application providers to be the mechanism for obtaining

information. How does an IPAR concept impact both present and future legislation relative to IP address information, internet activity, and subscriber protection? Let's review some current legislation and the impact to them in an IPAR implementation.

Laws established in Nevada and Minnesota require Internet Service Providers to keep information regarding their customers private, unless a customer specifically approves their information can be given out¹³. In a retail environment, stores can link your transactions through various databases and record your name, purchase trends, credit status, even the shelves you are more likely to purchase from. This law was intended to prevent ISPs from participating in this collaboration of subscriber purchases, in particular where a majority of commerce was shifting to online transactions. Whenever a consumer visits a website, makes a purchase or searches for information, that activity can be linked to the specific person. ISPs have far greater access to this information because the information is traveling across their network and comes from customers who are granted access through their IP subscriptions. These laws do not change with the IPAR. ISPs must continue to protect the confidentiality of their subscribers' activity. Instead the IPAR redirects activity monitoring back to the policing agencies further supporting this law for privacy protection.

In similar rulings, the New Jersey Supreme Court issued an opinion on the privacy rights of computer users, that computer users have a reasonable expectation of privacy concerning the personal information they give to their ISPs. The New Jersey Supreme Court ruled that ISP

¹³ Blanke, Jordan M. "Minnesota passes the nation's first Internet privacy law". Rutgers Computer & Technology Law Journal, <http://www.entrepreneur.com/tradejournals/article/106474530.html> (accessed September 26, 2010).

subscriber records can only be disclosed to law enforcement upon the issuance of a subpoena¹⁴. While the IPAR reduces the need for the subpoena to the ISP, law enforcement would not be able to obtain personally identifiable information unless first being granted permissible use to the repository. This protection of personal information can continue to be supported under an IPAR design as the user's personally-identifiable information remains secured and only the database that houses the information is changed.

In a similar manner, Minnesota also prohibits Internet service providers from disclosing personally identifiable information. The Minnesota laws include a consumer's physical or electronic address, telephone number, Internet or online sites visited, or any of the contents of a consumer's data storage devices¹⁵. They offer provisions under certain circumstances where information must be disclosed, such as to a grand jury, to a state or federal law enforcement officer acting as authorized by law, or pursuant to a court order or court action. This is legislation that can be fully supported under an IPAR implementation. The IPAR helps define the segregation of duties between the provider of the service and the keepers of record. Pursuant to investigation and judicial request, the IPAR provides authorities with access to tie an IP address to a user, while policing agencies link internet use to criminal activity.

¹⁴ O'Connell, Kelly. "Internet Law – NJ Supreme Court Says Subpoena Needed for Internet Records." *Internet Business Law Services*. http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2043 (accessed September 26, 2010).

¹⁵ Blanke, Jordan M. "Minnesota passes the nation's first Internet privacy law." *Rutgers Computer & Technology Law Journal*. <http://www.entrepreneur.com/tradejournals/article/106474530.html>. (accessed September 26, 2010).

As outlined in previous pages, the parliament of the United Kingdom passed the Digital Economy Bill¹⁶ earlier this year. Here is a law that is controversial because it is among the first to dictate that monitoring of subscriber activity as a task for the ISPs. Not only were ISPs required to monitor their subscribers' activities but they were also required to prevent access for users identified as engaging in criminal activity on the internet. For the first time, service providers are mandated as having both the policing and punitive roles. The ruling is mired with a lack of definition. How does the service provider differentiate between appropriate versus inappropriate activity? If certain sites are *always* 'inappropriate', wouldn't it be easier for the ISP to simply block them and prevent the monitoring, logging and reporting that would come along with them? The implications for both ISPs and subscribers are concerning.

The IPAR eliminates the need for such legislation for service providers in the United States. Law enforcement agencies with the training and skills needed for policing are empowered to police by being granted access to IP information when it is determined to be needed. Instead of logging millions of transaction records for all subscribers' activities in the event one engages in criminal activity, the criminal activity is identified first, then the subscriber that is engaging in that activity is identified and monitored. It is a more efficient use of systems and provides the delineation between the highway and the traffic cops.

Other legislative reforms have touched areas such as record retention, censorship, and 1st Amendment rights such as the freedom of speech. In 1996 the Electronic Communication Transactional Records Act was passed by Congress. While this Act covered the right of the

¹⁶ Parr, Ben. "UK Passes Controversial Digital Economy Bill." <http://mashable.com/2010/04/07/digital-economy-bill/>. (accessed October 3, 2010).

Federal Government (or governmental entity as described in the ECTRA) to request the contents of electronic or wired communication from ISPs, it also established guidelines for the length of time requested records would be retained¹⁷. Typically that retention period is defined as 90 days for any records requested via subpoena or court order from a service provider. If a legal entity requests data via court order, not only is the ISP required to respond to the request, the response and accompanying data must be preserved for a period of 90 days after the request is fulfilled. This is different than the historical two year retention of subscriber data. The two year record retention period means a legal entity can make reasonable assumptions that a subscriber's information will be available for the previous 24-month period. This directive means a request of subscriber information dated 12/25/10 should produce records on this customer that go back to 12/25/08. While the 90-day retention period would continue unaltered with the IPAR, the two year retention period would no longer be needed.

Even with the IPAR, the preservation order relative to subscriber data or subscriber activity remains as a mandated area of compliance when records are subpoenaed. Legal proceedings can take many months or even years to conclude thus there cannot be a risk of loss of data for anything requested in a legal case. Regardless of the existence of the IPAR, the 90 day retention period must be upheld. The IPAR, however, does negate the need to keep two years worth of subscriber IP data. This would now be redundant data to what exists within the IPAR. The implications from a legislative perspective would alter portions of the Electronic Transactional Records Act. One specific example for data retention guidelines states: "*Data*

¹⁷ US Department of Justice. 18 U.S.C. 2703. Requirements for Governmental Access. <http://justice.gov/criminal/cybercrime/usc2703.htm> (accessed September 30, 2010).

should be retained in such a way as to avoid their being retained more than once...¹⁸ This emphasizes the redundancy of the data now being maintained in the IPAR and support for the retention requirements to move to an IPAR-only requirement.

Other legislative guidelines are less defined. Several reforms, such as the Electronic Communication Privacy Act (ECPA)¹⁹ and the United States Cable Act (CA)²⁰ try to incorporate rules for notification when subscriber identifiable information is provided to law enforcement agencies. The establishment of the IPAR would drastically alter this principle and force changes to these notification provisions. With the Cable Act established in 1984 as a method to regulate cable services, it was not prepared for the transition that occurred when cable providers transitioned to providing internet services over their hybrid coaxial fiber networks. As such, under the Cable Act, there are definitions outlined when breaches occur relative to customer information, however there are not specific provisions relative to internet services or customer specific information in relation to internet usage through the cable provider. There is, however, guidance dictated under the Electronic Communication Privacy Act, which is more specifically directed to any provider who ‘sends or receives electronic communication’²¹. Considering that this Act was established in 1986, the definition of ‘electronic communication’ during the last 25

¹⁸ DCS.com. “Scope and impact of the European Data Retention Directive.” 16 January 2007. http://datacentresols.com/news_full.php?id=9515&title=Scope-and-impact-of-the-European-Data-Retention-Directive. (accessed September 29, 2010).

¹⁹ US Department of Justice. “Electronic Communications Privacy Act of 1986.” *Justice Information Sharing*. <http://it.ojp.gov/default.aspx?area=privacy&page=1285>. (accessed October 3, 2010).

²⁰ Epic.org. “Cable TV Privacy Act of 1984.” *Electronic Privacy Information Center*, http://epic.org/privacy/cable_tv/ctpa.html. (accessed October 11, 2010).

²¹ US Department of Justice. “Electronic Communications Privacy Act of 1986.” *Justice Information Sharing*. <http://it.ojp.gov/default.aspx?area=privacy&page=1285>. (accessed October 3, 2010).

years has changed drastically. While district courts are still divided on whether these acts still meet the needs of the present technology, they differ in what is defined for notification processes relative to customer private information. The CA defines notification requirements whenever information is provided to law enforcement. The other, the ECPA, defines that notification is not required and providers are exempt from liability. Which one then applies to present day service providers and would either apply to the IPAR?

Looking at a recent copy of Comcast Corporation's Customer Privacy Notice, the policy makes specific reference to the Cable Act as follows: *"As a subscriber to cable service or other services provided by Comcast, you are entitled under Section 631 of the federal Cable Communications Policy Act of 1984, as amended, (the "Cable Act") to know the following²²:*

- *the limitations imposed by the Cable Act upon cable operators in the collection and disclosure of personally identifiable information about subscribers;*
- *the nature of personally identifiable information we collect;*
- *the nature of the use of personally identifiable information;*
- *under what conditions and circumstances we may disclose personally identifiable information and to whom;*
- *the period during which we maintain personally identifiable information;*
- *the times and place at which you may have access to your personally identifiable information; and*
- *your rights under the Cable Act concerning personally identifiable information and its collection and disclosure.*

²² Cox Communication, Inc. "Cox Communication LEA Information Policy", last modified October 1, 2009. *Notice to parties serving subpoenas on Cox Communication*. <http://cryptome.org/isp-spy/cox-spy.pdf>. (accessed October 1, 2010).

Comcast's privacy notice goes on to reference the federal Telecommunications Act of 1996 and includes the following verbiage:

"In addition, Section 702 of the federal Telecommunications Act of 1996, as amended, (the "Telecommunications Act") provides additional privacy protections for certain information related to our phone services:

- *information about the quantity, technical configuration, type, destination, location, and amount of your use of the phone services; and*
- *information contained on your telephone bill concerning the phone services you receive.*

That phone information, when matched to your name, address, and telephone number is known as customer proprietary network information or CPNI for short. This notice, which includes our CPNI Policy, describes what CPNI information we obtain, how we protect it, and how it may be used. If you are a customer of our phone services, you have the right, and Comcast has a duty, under the Telecommunications Act, to protect the confidentiality of CPNI.²³

A full copy of Comcast Corporation's Privacy Notice is included in Addendum B.

While there are multiple legislative references in this privacy policy example from Comcast, the primary reference point for the treatment of confidential data in this document is the Cable Act. A fully functioning IPAR now implies changes not only to the definitions within these defined rulings, but also in numerous privacy policy statements that make reference to their compliance with these notification policies.

For customer notification principles in relation to the IPAR, the most applicable approach is for customers to be made aware that the IPAR exists. While information about a customer's internet usage is not disclosed, their IP information is being sent to database that law enforcement can access at any time. Again using the motor vehicle analogy, citizens are aware

²³ Cox Communication, Inc. "Cox Communication LEA Information Policy", last modified October 1, 2009. *Notice to parties serving subpoenas on Cox Communication*. <http://cryptome.org/isp-spy/cox-spy.pdf>. (accessed October 1, 2010).

that their license and vehicle information is contained in the DMV database and is available for law enforcement to access at any time. The principle with the IPAR would be no different.

Consumers are made aware of the existence of this new application and that the scope of access is restricted only to approved law enforcement and governmental agencies. Wording within legislative texts would have to be modified to outline specifications for conformity with the IPAR and this new compliance requirement for service providers. Modifications to individual privacy policies would then outline the ISPs mandate for submission to the IPAR, the ISPs ongoing protection of the confidentiality of consumer information, and specifications of IPAR restrictions for use to law enforcement.

Following typical guidelines for privacy policies, here are some expected changes that would be relevant to each section of a privacy policy once the IPAR is implemented:

- Describe what information is being collected online. Under this heading there would be a change to specify the collection of IP address information. The Comcast example outlines the collection of name, service/billing address, e-mail address, telephone number, driver's license number, social security number, bank account number, credit card number, and 'other similar account information'. IP Address should be listed as specific collected data. While it *could* be assumed to be included under the 'other similar account information' heading, it would be more appropriate to list it individually given the nature of IP address confidentiality concerns.
- Describe how collected information is shared. Here changes would outline how IP data is fed to the IPAR and the regulatory requirements to do so. Data is shared automatically, at the time the IP address is assigned, and shared to a secure federal and / or state mandated repository for law enforcement and governmental purposes.
- Describe choices available to consumers regarding marketing use of this collected information. There should be no marketing use for a consumer's IP address thus this should be specifically outlined. While other information such as name, address, and phone number may be provided for marketing purposes, and is specifically defined in this section, IP address information would not be included in that distribution. This

would follow similar treatment for non disclosure of customer social security number information for marketing purposes. As for choices to consumers, there is no option to 'opt out' of submission to the IPAR so specifics on opt-out options would have to delineate the exception for IPAR submission.

- Describe the consumer's right of inquiry about their own information. Typically consumers can request copies of their own information from service providers including copies specific to the individual privacy policy. This would be true of the IPAR as well. Consumers would have the ability to request their own records from the IPAR, in the same way consumers can request copies of their driving records from the Department of Motor Vehicle. Verbiage specific to this option for consumers should be outlined in this section of the privacy policy including links for the consumer to request such IPAR data.
- Describe how personal information is protected online. This section remains consistent with existing privacy statements and should not require modifications to accommodate the IPAR.

The changes documented here help to outline how far reaching the IPAR would be relative to existing legislative policies and company guidelines on compliance with these policies. Another example is the Customer Proprietary Network Information or CPNI as referenced in the above Comcast privacy notice. CPNI requirements were implemented as part of the 1996 US Telecommunications Act²⁴. Modifications to this act gave the Federal Communications Commission (FCC) the sole authority for determining how to regulate the use of information collected about a consumer's telephone calls. While this new consumer protection order was intended to cover items that are commonly found on any telephone bill such as the time, date, destination and duration of every call, it targets specific use of this collected data by telephone providers and how or if it can be shared. Similar to the Cable Act, this legislation was originally

²⁴ Federal Communications Commission. "Telecommunications Act of 1996." <http://www.fcc.gov/telecom.html> (accessed October 4, 2010).

targeted at telephone carriers who were, at that time, providing primarily copper-based, hardwired telephone services. As a majority of the carriers migrated to IP-based networks and services, certain portions of this CPNI definition remained stagnant and required modification. A common argument on the VoIP architecture refers to the IP address and corresponding mac address that are both part of the initiation session for a call. As such, do IP and mac address information fall under CPNI protection guidelines specific to telephone communication? If so, how does the existence of the IPAR modify the text of the existing rules?

The privacy policy of RidgeviewTel LLC provides a good outline of how CPNI and IP address data can be combined into one consolidated form. Their policy states: *“Every computer connected to the Internet is assigned a unique number known as an Internet protocol (IP) address. Since these numbers are usually assigned in location-based blocks, an IP address can often be used to identify the area from which a computer is connecting to the Internet. This information can be used by governmental authorities or RidgeviewTel for legal purposes such as tracing criminal acts and responding to emergencies.”*²⁵ A policy such as this does provide disclosure to the consumer as to how IP address information can be used. While the IP address is not defined specifically under CPNI rules, it does fall under CPNI guidelines when it is married to customer identifiable information, and this is exactly what the IPAR does. As such, this would indicate that the IPAR should fall under those same legal requirements. It opens an interesting prospect of the government having to regulate itself if they are the ones that ultimately own the IPAR data.

²⁵ RidgeviewTel™ LLC. “Privacy Policy”. <http://www.myridgeviewtel.com/site-policy.php> (accessed December 27, 2010).

Migration to IPv6

A majority of the addressing process in use today, and outlined here, is specific to the current world-wide implementation of IPv4. As the 'v4' indicates, our present IP standard is based on the fourth version of IP deployment. This standard, as outlined in RFC791, was defined in 1981 and is based upon a 32 bit address, made up of four 8-bit octets.²⁶ The four octets are used together to define IP address classes, and further determine bit allocations for network and node designators within the 32 bits. Using this combination of network and host bits, IPv4's 32 bit address can support more than 4 billion unique, usable IP addresses. While this seems like a sufficiently large number, when dissected across the global internet it is not nearly enough to support all users or systems. Considering the top 5 countries with the highest number of internet users, as shown in the table below, this range of addressing in IPv4 is shown to have already been exceeded in just China alone:

TOP 5 COUNTRIES WITH HIGHEST NUMBER OF INTERNET USERS						
Ranking	Country	Population, 2010 Est	Internet Users Latest Data	% Population (Penetration)	Growth 2000-2010	% of World Users
1	China	1,330,141,295	420,000,000	0.32	17.67	0.21
2	United States	310,232,863	239,893,600	0.77	1.52	0.12
3	Japan	126,804,433	99,143,700	0.78	1.11	0.05
4	India	1,173,108,018	81,000,000	0.07	15.20	0.04
5	Brazil	201,103,330	75,943,600	0.38	14.19	0.04
TOP 5 Countries		3,141,389,939	915,980,900			

*NOTES: World Internet User Statistics were updated for June 30, 2010. The most recent user information comes from data published by Nielsen Online, International Telecommunications Union, Official country reports, and other trustworthy research sources. Data from this site may be cited, giving due credit and establishing an active link back to Internet World Stats. Copyright © 2000 - 2010, Miniwatts Marketing Group. All rights reserved.*²⁷

²⁶ Information Sciences Institute, University of Southern California. *Internet Protocol. Darpa Internet Program Protocol Specification.* <http://www.ietf.org/rfc/rfc791.txt> (accessed January 2011).

²⁷ World Internet Usage Statistics News and World Population Stats. "Internet Usage Statistics, The Internet Big Picture." <http://www.internetworldstats.com/stats.htm> (accessed October 11, 2010).

This means the migration to the next version of IP addressing, IPv6, is inevitable, and in actuality fast approaching. What does this upcoming transition to IPv6 mean to an IPAR implementation and does this migration have positive or negative impacts to its deployment? Let's start by looking at the inherent differences between IPv4 and IPv6.

IPv6 extends the IP address from 32 bits in IPv4 to 128 bits. This means if IPv6 was fully deployed across the entirety of Internet / network space, it would support 3.4×10^{38} usable IP addresses, or 3.40 undecillion (36 zeros) addresses. While this exponentially expands the distribution of IP addresses available for use, it also changes the format of IP addresses. IPv4 addresses are configured in the 32 bit, dotted decimal notation we are now familiar with: 192.168.2.10 which translates at the bit level to 11000000.10101000.00000010.00001010. IPv6 uses a completely different format for the IP address, breaking the address into eight 4-digit hexadecimal octets, separated by colons (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx). Because the address is hexadecimal as opposed to binary, the x values in the address can range from 0's to f's (0000 – ffff) or up to 16 different values per x placeholder. Comparing an IPv4 address to its new IPv6 format we see:

```
IPv4: 192.168.2.10
IPv6: 2002:COA8:20A:0:0:0:0:0
```

If this IPv6 was then transcribed into an URL for use on the internet it would appear as:

```
http://[ 2002:COA8:20A::]:80/index.html
```


So what does this mean to the IPAR? Foremost, it means the IPAR must be able to support both the syntax of the IPv4 address as well as the IPv6 address format simultaneously. The transition to IPv6 can be time-consuming, having to configure all devices to the new protocol, and does not come without upgrade costs as older devices and software may require upgrading to support IPv6. As such, the transition to IPv6 will not be a quick one, but will instead be a migration that occurs over a considerable period of time. This means the systems to support the IPAR must also be fully IPv6 compatible and also able to support incoming data that is either IPv4 or IPv6 based.

The impending transition to IPv6 means the IPAR must also be sized to accommodate the growing number of IP-based users expected in the next 10 years. Considering only subscribers in the United States, the previous table shows nearly 240 million internet users as of June 2010. At the date of inception of the IPAR, it would need to be sized to support at least half of those records. This number is based on the point in time that the database is live to the time it takes for providers to modify their systems to direct IP changes to it, as well as the number of changes to subscriber's information that will occur from that point in time forward. Next, assuming these users changed their IP addresses only one time in the first year, the IPAR would have to support a possibility of 200 million records in short order. Given that the true number of IP address changes per subscriber is much higher than one per annum... having to account for new users, moves, service changes, periods of inactivity, and system upgrades... the sizing of the IPAR is significant. The transition to IPv6 itself will generate significant numbers of address changes for subscribers which would need to be reflected within the sizing of the IPAR.

Wireless Migration to 4G

Looking forward only 10 years, we need to consider the changes to the wireless industry that are making it the new industry standard for 'any service anywhere'. The growth of wireless mobile devices continues to grow exponentially as users transition away from hardwired systems to go-with-you applications. Service providers are merging IP into telephony, video and other applications. Start a movie at home, and watch it on your cell phone as you leave home. Surf the internet on your TV. Integrate your VoIP home phone to your cell phone, to your computer, to your TV. This isn't a world of tomorrow; it is the reality of today. What it means at the technical level is that more and more applications are moving to IP space and mobile providers are transitioning to all-IP deployments.

The current platform for wireless service is based upon 3G technology, or the third generation of mobile environment. 3G was originally based upon the telecommunication industry, most specifically the traditional telephony carriers, and their existing circuit switched cellular networks. While good for providing for its generation of mobility, it was based on an older and slower technology. The newer, fourth generation network or 4G, is based on a packet switched network which offers higher speeds and greater integration of services and applications.

Packet switched networks are IP based, using source and destination addresses in small sized packets to route data across networks from one node to another. Implementing this into the wireless space means a greater integration of applications to mobile devices and exponentially expanded use of IP addressing in the wireless world. The impending migration to 4G means the ultimate transition to an all-IP based wireless environment.

Why is the migration to all-IP important in the wireless space and how is this relevant to the IPAR? Consider the number of IP addresses in use in the typical home environment. A subscriber receives a modem from their provider which requires, by itself, one IP address. The subscriber is then generally provided with up to 5 usable IP addresses. This is a fairly static value, providing for connectivity to one or two PCs, a gaming system, and perhaps an Internet capable TV. Once assigned and configured for use through the provider, the number of IP addresses cannot be exceeded and the lease duration of these IP addresses is fairly stagnant. The wireless realm operates a bit differently.

As is true of wired ISPs, IP address scopes vary by provider. In a 4G world each mobile device is provided an IP address from its carrier, but that mobile space is shared from one provider to the other. This shared mobile space allows a user to drive from one end of the country to another and maintain reasonably stable connectivity as they transition from one provider to the other, from one cell tower to the next. As the mobile user transitions from one carrier network to another, their IP address moves along with them.

The most notable relevance of this migration to 4G networks is that this technology enables the convergence of the wired networks to wireless. IP-based applications and services that had been, for the most part, isolated to the wired network are now fully functional in the realm of the mobile device. The adaptation of this new generation of technology only heightens the

depletion of IPv4 address ranges and hastens the requirement for full migration to IPv6. New specifications of 4G devices require IPv6 addressing²⁸.

An IPAR system offers significant improvements to wireless providers. Data requirements for this subset of providers can be more involved than for traditional wired providers. For a typical ISP, personally identifiable information for a subscriber consists of the IP address in use and the physical address on file for that subscriber. Though that is also true of the wireless subscriber... this IP address is assigned to this customer at this address... the subscriber is mobile thus their actual location will vary. For the purposes of successful law enforcement, the identifiable information for the physical location where the activity originated can be difficult to obtain. If an internet crime takes place for a wired customer, it is fairly easy for law enforcement to obtain the location of the activity from the provider. When that internet crime takes place on an IP enabled mobile device, the positioning location of the device can be an important component of law enforcement's investigation. As outlined in an interview with Sergeant Glenn Lang of the Maine State Computer Crimes Unit, *"..in our typical child pornography case the location is secondary by far to the name of the subscriber. In most of these cases the location is not very important because they generally need or want privacy to upload or download contraband. That is almost always home. If it's a harassment or missing person case the location is the vital part of the investigation. Wireless devices in general have created a lot of problems for us..."*²⁹

²⁸ Wikipedia.com. "IPv4 address exhaustion." http://en.wikipedia.org/wiki/IPv4_address_exhaustion (accessed December 27, 2010).

²⁹ Lang, Glen. Phone interview. Sergeant Glen Lang, Maine State Computer Crimes Unit. (6 Oct. 2010).

Sergeant Lang outlines an important separation in information needed between the wired and wireless worlds. As such, an IPAR would either have to account for both scenarios, as both will be submitting data to the repository, or provide alternative methods separating the two types of providers. As previously indicated, for traditional wired ISPs location information will consist of the address on file for the subscriber. For wireless providers, the location information would include similar data relative to the physical address of the subscriber, however, location information relative to the mobile positioning of the cellular device when the IP address was assigned would have to be either appended as part of the data stream or omitted and provided in a separate request.

To determine the best approach for this discrepancy in location information, let's go back to the original concept of the IPAR. The IPAR is based on a similar model to a freeway, toll charges, and vehicle license plate information. These represent the Internet (freeway), the service provider (toll charges) and the web-enabled user (license plate). Highway users are mobile in the same way wireless customers are mobile. The highway authority is not concerned with the location of the cars on the highway, only that they have paid the toll fees to use it. Law enforcement is the entity concerned with location of the vehicles, but like the toll taker, they are not concerned with the location of *every* vehicle on the highway as this is far too much data for them to digest. Instead they are concerned with the location of the vehicle *only when an incident occurs*. This lends to a sound conceptual approach to the IPAR. Location of the subscriber, or in this model the address of the vehicle's registration, is a mandatory inclusion in the data stream from the provider to the IPAR. Various mobile locations of the subscriber are too changing and would overburden the IPAR when the mobile location is really only important

when an incident occurs. As a method to avoid collecting millions of unnecessary records for wireless providers, the positioning location information for the mobile user would not need to be fed real time to the IPAR. This information would continue to fall under the standard subpoena process and be requested only when needed, only when an incident or event warrants this information relative to investigation. This method enables a uniform format for the data feed to the IPAR regardless of provider. Law enforcement would still have real-time access to the owner/user of an IP address and could subpoena additional information from the provider when needed.

This continued migration to 4G by the wireless carriers offers these carriers added benefits from the existence of an IPAR. As outlined above, the transition from 3G to 4G technology represents the continued transition from circuit-switched to packet-switched technology. This is the migration from the traditional telephony carrier model to the IP-enabled internet model. Mobile devices are completing their migration from cellular telephony devices to internet enabled, application converged devices. These are no longer phones but instead are small portable computers. This is an opportune time for an IPAR implementation.

Looking back five years ago, Verizon Wireless would have been subpoenaed for phone records. The future for Verizon will include being subpoenaed for internet usage records of their mobile devices. Instead of continuing to develop high capacity systems internally to support this changing data and meet this new data retention model, they could instead feed subscriber IP information to the IPAR.

The Implementation

With the conceptual model of the IPAR defined, the next step in its development is the determination of the sizing and ultimate feasibility of the actual operating model. This outline needs to account for the number of transactions, their content, systems sizing and database components. As with any database, there is a threshold between storage and retrieval where there is an incremental degradation in functionality when the number of records grows so large that indexing and lookups become too delayed for reasonable use. This balance between storage and retrieval has to be accounted for in the design as this is inherently going to be a very large database. There must also be methods to ensure high levels of security given the sensitivity of the data and the targeted segment of users that will be allowed access to the data. As defined above, there should also be accommodations for the long term migration to a full IPv6 environment, meaning the system must be able to support two distinct IP record formats for the unforeseeable future. Finally, every backend data storage system needs an intuitive front-end interface that makes retrieval of the data fast and easy and geared toward the users who will be using it.

For the IPAR implementation let's begin with sizing. Based on data from June 30th, 2010, the Internet Usage and World Population Statistics reported there were 239,232,863 internet users in the United States³⁰. Where the IPAR is intended only for the United States and is not a global endeavor, this value of approximately 240 million users would be the basis for preliminary

³⁰ World Internet Usage Statistics News and World Population Stats. "Internet Usage Statistics, The Internet Big Picture." <http://www.internetworldstats.com/stats.htm> (accessed October 11, 2010).

sizing. Keeping in line with our motor vehicle registration analogy, there were 255,917,664 registered vehicles in the United States according to the 2008 Bureau of Transportation Statistics. In comparison, these values are close enough to speculate that if an existing system can support our vehicle registration data then one likely could be sized to support IP address assignments. The scope for sizing is still within range of reasonability.

When we begin to look at the changeability of the data the systems begin to diverge. According to R. L. Polk & Co. the average American keeps their vehicle for 63.9 months or 5.3 years.³¹ Americans change their vehicles exponentially less often than they change IP addresses. This means the motor vehicle database, which contains a similar number of users, contains data that is relatively stagnant when compared to the changeability of IP address data. Studies from 2008 indicate that the average PC in the United States uses 5.7 distinct IP addresses per month.³² While this 5.7 value represents only 40% of PCs (with the other 60% maintaining much more stable IP addressing) these systems that changed their IP address during a month did so with great frequency. The differentiation here is that the sizing for the IPAR has to accommodate not only a formidable amount of data but frequently changing data as well.

In the technical realm of database technology, there is a term known as VLDB or Very Large Database. This terminology helps to define databases that grow well beyond the size of the average operating database. Wikipedia provides the following definition: “A *very large*

³¹ Korzeniewski, Jeremy. Nov 5, 2010. “Polk: People continuing to keep vehicles longer.” <http://www.autoblog.com/2010/11/05/polk-people-continuing-to-keep-vehicles-longer/>. (accessed December 13, 2010).

³² Meierhoefer, Cameron. October 12, 2010. comScore Voices. “comScore September 2010 qSearch Reporting Enhancements.” <http://blog.comscore.com/meirhoefer.html>. (accessed December 13, 2010).

*database, or VLDB, is a database that contains an extremely high number of database rows, or occupies an extremely large physical file system storage space. The most common definition of VLDB is a database that occupies more than 1 terabyte or contains several billion rows...*³³

Given the scope defined for the IPAR thus far, it meets these criteria as a VLDB. There are a variety of hardware and software platforms that can support VLDBs and these include standard server applications such as Microsoft SQL Server and Oracle. These applications primarily reside on Windows or Sun based servers supporting a client/server database environment. Microsoft SQL specifications outline support for a maximum database size of 524,272 TB of data, 32,767 user connections and a maximum number of rows limited only by the storage capacity of the hard drives within the server hard drives or storage network.³⁴ This would support the preliminary sizing for the IPAR. For very large scale applications, however, mainframe architecture is often the selection of choice and is, not coincidentally, the platform in use by the Department of Motor Vehicles today. Let's look at why.

There are several features of the mainframe environment that make it the ideal platform for a system like the IPAR. Reliability is one significant benefit. This comes grouped into a set of native features known as RAS which stands for Reliability, Availability, and Serviceability.³⁵

While the acronym is now commonplace, it describes one of the most purposed reasons the

³³ Wikramanayake, G.N. and J.S. Goonetillake. "Managing Very Large Databases and Data Warehousing." University of Colombo School of Computing. <http://www.cmb.ac.lk/academic/institutes/nilis/reports/gihan.pdf> (accessed December 22, 2010).

³⁴ Microsoft Corporation©. 2011. "Maximum Capacity Specifications for SQL Server." [http://msdn.microsoft.com/en-us/library/ms143432\(printer\).aspx](http://msdn.microsoft.com/en-us/library/ms143432(printer).aspx) (accessed November 12, 2010).

³⁵ Lie, David and John Maly. Stanford University. May 27, 2000. EE482: "Advanced Computer Organization Processor Architecture." *Reliability, Availability, and Serviceability*. <http://cva.stanford.edu/classes/ee482a/scribed/lect16.pdf> (accessed November 12, 2010).

mainframe environment continues its stronghold in the database market. The system architecture offers one of the greatest uptime values in the market.³⁶ This is achieved through various techniques of malfunction self-detection and continued operation through system hardware or operating system errors. Considering the always-on nature of the internet and the collective use of the IPAR to capture that IP data, the system that houses the IPAR must offer the highest uptime and availability possible.

Another advantage of the mainframe environment is security. In 1991 an international standard for security went into effect known as the Evaluation Assurance Level (or EAL 1 – 7)³⁷. This EAL value is assessed on technology applications or systems with a numeric grading assigned once a Common Criteria security evaluation is completed. IBM's mainframe platform received one of the highest levels of security certifications, EAL Level 5.³⁸ While the numerical designate is indicative of successful security testing, there are also other factors that provide native security advantages to the mainframe platform. By its very platform the mainframe is more secure than traditional environments like Microsoft. Consider it the hackability quotient. There are far fewer programmers that possess the necessary skills to hack a mainframe environment than those that can hack a Microsoft environment. Microsoft's platform leaves many holes through which a hacker can attack, erase, or siphon information and there are many more programmers with the skills and tools to impact that environment. In a January

³⁶ Radding, Alan. July 22, 2010. Big Fat Finance Blog. "Mainframe 101 for C-Level Executives." <http://bigfatfinanceblog.com/2010/07/22/mainframe-101-for-c-level-executives/> (accessed November 12, 2010).

³⁷ Wikipedia. "Evaluation Assurance Level". http://en.wikipedia.org/wiki/Evaluation_Assurance_Level (accessed November 12, 2010).

³⁸ IBM®. "IBM Security." <http://www-03.ibm.com/systems/z/advantages/security/index.html> (accessed November 12, 2010).

2010 article by Stan King titled “Mainframe Hacking: Fact or Fiction” he assesses mainframe security well:

“If you want proof of this claim, consider what you can find by searching news archives and trade journals, looking for references to mainframes and data loss, hacking, security breaches, and similar topics. Recent research included checking the archives of ComputerWorld, InformationWeek, and The Wall Street Journal for reports of unauthorized access of any traditional mainframe environment via userid/password exploitation, corruption of a mainframe-based networking resource, or contamination of a mainframe system software component. This list may sound decidedly short, but it represents the basic foundation of mainframe safety, security, and integrity..... all computers aren’t created equal.”³⁹

Security is likely the most important aspect of the IPAR implementation. This is a database containing sensitive information that is intended to be restricted to law enforcement and governmental agencies. Having a hardened system to support that data is imperative. This would be a similar evaluation that led to the mainframe in place in support of the motor vehicle database.

While security is critical, it is still imperative that the system be physically sized to accommodate not only the data it will store but the number of users who will access that data and the processing time it takes to index and access that data. Indexing of data is a critical function and one that relies more heavily on system memory than hard drive space. One

³⁹ King, Stan H. January 11, 2010. “Mainframe Hacking: Fact or Fiction?” <http://www.mainframezone.com/it-management/mainframe-hacking-fact-or-fiction> (accessed November 12, 2010).

common choke-point in very large databases is that indexing can become so large it fills system memory to capacity, reaching a threshold where data ultimately becomes inaccessible. The DMV model not only accounts for massive volumes of data and optimal security, the databases themselves are additionally distributed into state and/or regional systems. The format of the DMV model segregates both the registration management as well as the physical systems by state which reduces the size of any one database and further reduces responsibility to the subset of the drivers residing in the state. While each database can be queried through links to the others, this separation of databases reduces the size of each individual database, improves indexing and lookups having less data to sort through and also narrows the scope of data to keep it aligned with law enforcement's jurisdictional areas. This is an ideal model to emulate with the IPAR.

Again following the DMV's existing design, the IPAR system would be dissected into individual state systems. Each of these state-level IPARs would support the customers subscribing to internet service within each state. As an example, Time Warner Cable's New England division supports customers in Maine, New Hampshire, and Massachusetts⁴⁰. Under this model, Time Warner Cable would send IP data on their Maine customers to the Maine IPAR database, while sending IP address data on their New Hampshire customers to the New Hampshire IPAR. The records would contain a common ISPID (ISP ID) as the provider is the same for both states, however the records would be sent to two different systems based upon the physical location of the customer. This is a common delineation that ISPs use in scoping IP address ranges between states or metropolitan areas, keeping the structure of the IPAR in line with current ISP

⁴⁰ Time Warner Cable, Inc. Subscriber Statement. January 1, 2011.

and state operations. Furthermore, this model supports law enforcement entities that are typically limited jurisdictionally by state. This structure provides the most supportive model relative to data retrieval as the Maine police officer wouldn't have to query through millions of records from other states to obtain the data from their own. As is the case with the DMV and with law enforcement relative to criminal activity, any criminal actions that cross state lines falls under federal jurisdiction. Federal agencies would have access to all state IPARs.

The present DMV structure contains 51 separate state or territorial entities. This would then be a configuration baseline for the IPAR with one database per state. Law enforcement entities and state agencies would be granted specific access to their state's IPAR, with Federal and Governmental agencies being granted access to all IPARs.

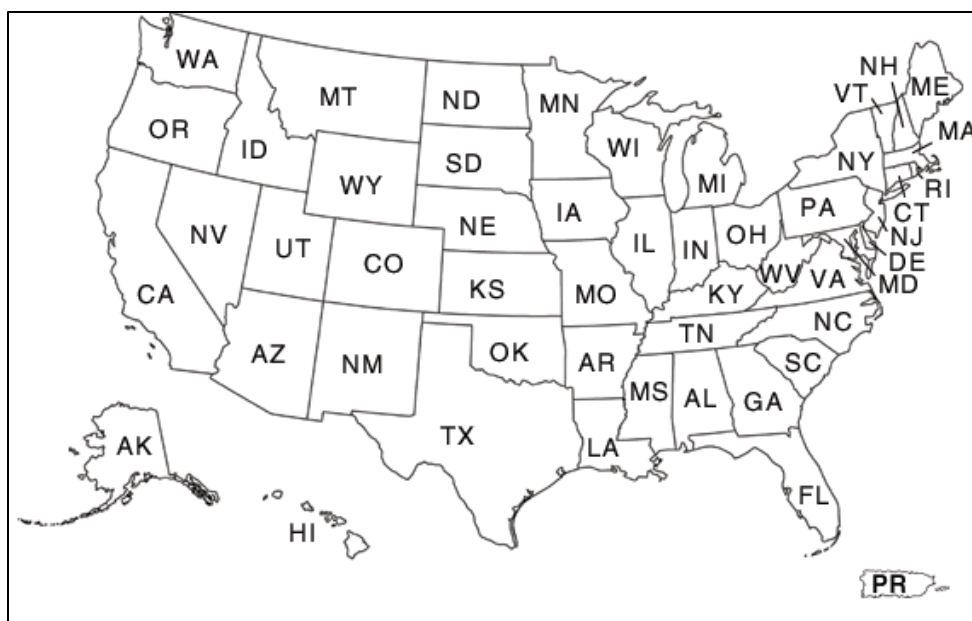


Figure2: DMV Geographic Agencies

With design and scope of the IPAR identified, our last systematic configuration would define the format of the data fed to and contained in the IPAR and the querying system that enables its access. Let's begin with record format.

IPAR Record Format

Every data string to the IPAR will begin with the ISPID field. This field represents the ID of the ISP that is sending the record and ultimately responsible for the IP assignment to the customer. This ISPID number will be contained in *Field 1* and is represented by a seven-digit numeric value assigned to the ISP when registering with the IPAR. Seven numeric digits in the ISPID means the field can support 10^7 unique ISP identifiers or 10 million unique values... more than enough to accommodate the number of registered ISPs in the United States.⁴¹ The first character in this ISPID number represents the geographic range of the ISP. 1 in the first position equates to an ISP that is wholly contained within and serving a single state entity (ex: Vermont). A value of 4 means the ISP serves only a single, unique metropolitan area, such as New York City or Los Angeles. A 7 represents an individual ISP that provides service across more than one state, as was the example referenced above for Time Warner Cable's New England division (Maine, New Hampshire and Massachusetts). All other values for the first character in the ISPID are reserved for future designations. The remaining 6 digits within the ISPID are sequentially assigned at the time of registration.

⁴¹ Internet World Stats Usage and Population Statistics. "United States of America Internet Usage and Broadband Usage Report" <http://www.internetworldstats.com/am/us.htm> (accessed October 11, 2010).

Field 2 in the IPAR data string, the Format Field, is a single-digit numeric value that represents the format of the IP address. A numeric value of 4 represents an IP address that is formatted as an IPv4 address. A numeric value of 6 indicates the IP address format is in the form of an IPv6 address. The delineation is important for various reasons. Foremost, the IPAR must be able to support both IPv4 and IPv6 for a period well into the future as both formats will exist concurrently for many years. In addition, the character length and format of the address varies significantly from an IPv4 address to an IPv6 address. This means that the following field, which will contain the actual IP address, will be a variable length, with the length of the field dependent upon the type of IP address being sent within the string. A precursor value designating the IP version of the address ensures proper interpretation and handling of the subsequent value. This also ensures an easy transition to the eventual all IPv6 environment when the Format Field can eventually be discarded or dropped.

Field 3 in the IPAR data string is the IP Address. This is a variable-length, alphanumeric field that will contain the IP address assigned to the customer.

Field 4 is an alpha field that contains the Last Name of the subscriber. This will be a fixed-width, left adjusted field, with a predefined field length of 30 characters.

Field 5 is an alpha field that contains the First Name of the subscriber. Like *Field 4*, this will be a fixed-width, left adjusted field, with a predefined field length of 30 characters.

Field 6 in the IPAR string is the zip code field and contains the zip code of the service address for the subscriber. This will be a numeric field set to a fixed width of 5 characters. The zip code

provides additional methods for subscriber delineation and can accomplish this in a few ways. Of greatest importance, the zip code can provide a primary level of jurisdiction. In the example above, where the single ISP provides service across multiple states, a zip code check point ensures data can be segregated out to the appropriate policing authorities. A zip code for a Maine subscriber can be distinguished from that of a New Hampshire subscriber, separating those into the proper IPARs and proper jurisdictional entities. In addition, a zip code further distinguishes subscribers who may share a common first and last name, such as Mary Brown. For a police investigation, narrowing the field for inquiry is critical. When there is a trigger for criminal activity, it is important that law enforcement is able to narrow their focus down to the appropriate geographical area. In a metropolitan area such as New York City, that has 176 unique zip codes⁴², this is a valuable piece of additional information in reducing the scope of an investigation. When used in conjunction with the leading digit in the ISPID address, which designates the geographic range of the ISP, law enforcement enjoys better optimization of this repository.

Field 7 is the Date Field and indicates the date that the IP address was assigned to the customer. As a date field, this field is formatted as an all numeric, 8-digit value, with a data format of YYYYMMDD, or 20101225. Keeping in mind the purpose of the IPAR is to provide as close to real-time data as possible relative to IP address assignments, this is intended to be a very accurate date value relative to the assignment and in an optimal configuration this data is sent to the IPAR at the time the assignment is made to the customer.

⁴² Yahoo Answers.com. "How many different ZIP codes are there in New York City?" <http://answers.yahoo.com/question/index?qid=20070320141640AAcuLmf> (accessed November 3, 2010).

Field 8 is the Time Field and represents the timestamp of the IP address assignment to the subscriber. All time values will be designated on GMT or Greenwich Mean Time standard⁴³.

9:30PM Eastern Standard Time would be represented as 02:30am GMT.

Integrating the above fields into a single data string, our format now appears as follows:

<ISPID>,<FormatField>,<IPAddress>,<LastName>,<FirstName>,<Zip>,<Date>,<Time>

The received data is interpreted in the table below.

ISPID	Format Field	IP Address	Last Name	First Name	Zip	Date	Time
7722651	4	192.168.2.10	Ouellette	Rita	04101	20101225	09:47:03
4722633	6	2002:COA8:20A:0:0:0:0	Brown	Mary	11040	20101107	22:01:11

This standard format for data submission to the IPAR means no header record needs to be sent prior to the transmission of the data string. When an IP address is allocated to a subscriber from a dynamic pool of IP addresses, this data string, in this format, is forwarded to the IPAR for registration within the database. Over a period of normal operations, this table is updated numerous times with the various changes in assignments for each customer. As the data is populated a record of a user's IP address assignments begins to emerge. Using the table below as a representation of the data fed into the IPAR, law enforcement and other IPAR users will have an accurate record of the historical IP addresses assigned to customers and for what period each user had the IP address for their use.

⁴³ Timeanddate.com. "GMT – Greenwich Mean Time."

<http://www.timeanddate.com/library/abbreviations/timezones/eu/gmt.html> (accessed November 3, 2010).

ISPID	Format Field	IP Address	Last Name	First Name	Zip	Date	Time
1895577	6	fe80:0:0:0:0:a59:4202	Oneida	Uda	13042	20100531	23:58:02
7775633	4	87.63.89.111	Haviezeh	Rameira	90210	20100720	10:28:11
7632478	4	128.7.63.9	Pike	Trenton	37201	20100819	17:33:59
4756352	6	fe80:0:0:0:0:ac6:4d59	Kincade	Rosaire	30301	20101001	11:31:45
4722633	6	fe80:0:0:0:0:c0a8:20a	Brown	Mary	11040	20101107	22:01:11
4722633	6	fe80:0:0:0:0:c0a8:216	Brown	Mary	11040	20101130	18:15:07
1777755	4	198.225.112.87	Lambert	Ralph	83728	20101113	13:45:19
1895467	4	30.250.17.95	Oda	Kathy	60601	20101118	12:02:02
1257963	4	21.225.78.53	Sanchez	Have	27609	20101125	19:05:05
1124590	4	45.6.211.9	Neal	Beverly	99501	20101201	6:12:54
7983219	4	10.198.22.56	Slate	Philip	06155	20101218	1:17:45
1257965	4	172.22.96.89	Gordone	Helen	28202	20101219	2:02:09
7722651	4	192.168.2.10	Ouellette	Rita	04101	20101225	9:47:03
...
...
...

Figure 3: IPAR Data

Query and Selection Application

In order for the IPAR tool to be truly usable in its intended manner, sorting and selection criteria will have to be developed into an easy-to-use query application. The IPAR application, or IPAP, will offer the following usability features:

- Three-factor authentication login window ensuring secure access to IPAR data.
- Data look-up functionality allowing for selection by Name (Last Name, then First), and IP Address
- Printing and saving functionality.

Two-factor authentication is the most common industry standard for authenticating users as they attempt to access secure data.⁴⁴ Any method that requires dual entry to obtain access can be deemed two-factor authentication; however, the truest forms incorporate the use of tokens or fobs for the most secure levels of access. For the IPAR Application (IPAP), three-factor authentication is defined and represented in the following login screen:

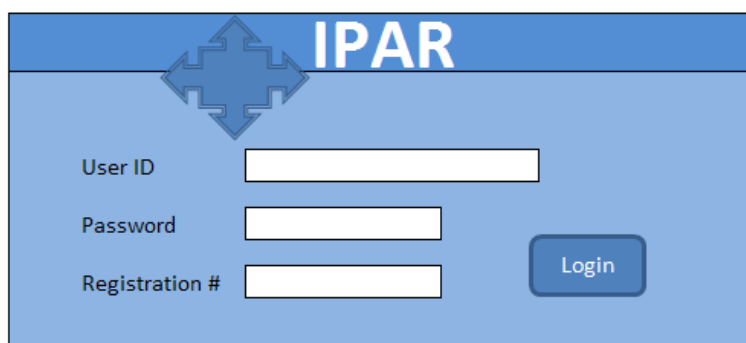
The image shows a login screen for the IPAR application. At the top, there is a blue header bar with a white cross icon and the text "IPAR" in white. Below the header, the background is a light blue color. On the left side, there are three labels: "User ID", "Password", and "Registration #", each followed by a white input field. To the right of these fields is a blue button with the text "Login" in white.

Figure 4: IPAR Login Screen

Remember that law enforcement must register with the IPAR in order to obtain access to the data. Only validated law enforcement and governmental agencies will be granted access to use the system. Upon successful registration, users are provided with a Login ID and a system generated, sequentially-assigned numeric Registration Number. Once prompted to create the initial password for the account, these three pieces of information must be entered in order to gain access to the IPAR.

⁴⁴ Bradley, Tony. About.com. "What is Two-Factor Authentication?" *Understanding what two-factor authentication is and how it works*. <http://netsecurity.about.com/od/quicktips/qt/twofactor.htm> (accessed November 14, 2010).

Data lookup functionality is then presented to the user. Users are offered the ability to sort by both Name and IP Address. The following image provides an example of the Name Query screen and the data presented:

Last Name	First Name	IP Address	Zip	Date	Time	ISPID
Brown	Mary	fe80:0:0:0:0:c0a8:20a	11040	20101107	22:01:11	4722633
Brown	Mary	fe80:0:0:0:0:c0a8:216	11040	20101130	18:15:07	4722633
Brown	Mary	fe80:0:0:0:0:c0a8:222	11040	20101219	6:06:17	4722633
Brown	Mary	fe80:0:0:0:0:c0a8:20c	11040	20101222	1:55:59	4722633
Brown	Mary	fe80:0:0:0:0:c0a8:223	11040	20101223	13:24:35	4722633
Brown	Mary	fe80:0:0:0:0:c0a8:02c	11040	20101228	18:11:22	4722633
Brown	Mary	fe80:0:0:0:0:ac6:4d61	99501	20101230	5:15:30	1124590
Brown	Mary	fe80:0:0:0:0:ac6:4d62	60601	20101231	11:25:02	1895467
Brown	Meagan	30.250.17.96	04072	20100914	2:33:01	7234501
Brown	Meagan	45.6.211.9	90210	20101010	9:32:45	1892671
Brown	Meagan	24.227.65.13	30301	20101002	12:01:55	4157236
Brown	Meagan	fe80:0:0:0:0:a59:4202	99501	20101114	7:17:27	1182695

Figure 5: IPAR Name Query Screen

Queried data is sorted by the name queried, in alphabetical order by Last Name then First Name. Names that are an exact match to the selection criteria are highlighted for easy recognition, with the remaining fields presented for further ability to narrow the selection to an individual record. Additional sorting presents each record in order by Zip Code, Date and Time. In this example, the first six records provide an outline of one customer and their IP Address assignments over a period of 55 days.

Similar processes are in use in selections by IP Address. The IP Address Query screen is shown below:

IP Address	Last Name	First Name	Zip	Date	Time	ISPID
30.250.17.96	Brown	Meagan	04072	20100914	2:33:01	7234501
30.250.17.96	Ruiz	Armando	04074	20101101	3:11:14	7234501
30.250.17.96	Clark	Michelle	04074	20101109	23:29:09	7234501
30.250.17.96	Hughen	Andrew	04072	20101118	22:18:57	7234501
30.250.17.97	Brown	Mary	04072	20101107	22:01:11	7234501
30.250.17.97	Buswell	Pamela	04074	20101130	18:15:07	7234501
30.250.17.97	Norton	Shawn	04074	20101219	6:06:17	7234501
30.250.17.97	Willis	Ramoe	04072	20101222	1:55:59	7234501
30.250.17.97	Gamage	Joe	04072	20101223	13:24:35	7234501
30.250.17.97	Lester	William	04072	20101228	18:11:22	7234501
30.250.17.98	Groton	David	04072	20101230	5:15:30	7234501
30.250.17.99	O'Donnell	David	04072	20101010	9:32:45	7234501
30.250.17.99	Maxwell	Raymond	04072	20101225	1:16:45	7234501
30.250.17.99	McNutt	Amy	04073	20101231	11:25:02	7234501

Figure 6: IPAR Address Query Screen

Selected data is presented in order by IP Address. Records matching the queried IP are highlighted for quick recognition. Data is then further sorted by the Date and Time of the assignment of the IP Address, providing a historical record of the assignment of this specific address. ISPID values remain the same on each record as this IP address block belongs to a specific service provider.

Within each query screen are the options to Print or Save the data results. This ability to make a permanent record of the queried data is critical in criminal investigations. Evidence must be available in a format that is admissible as evidence. Without proper accompanying data,

'screen shots' of data from a terminal are not viewed with the same quality rating as report data that has date and timestamp values within the report structure. Providing proper header information containing the IPAR designation along with the data and time of the report and subsequent data provides a highly credible record of the IP Address data for submission in legal proceedings.

Sample report data is shown here:

IP Address	Last Name	First Name	Zip	Date	Time	ISPID
30.250.17.96	Brown	Meagan	04072	20100914	2:33:01	7234501
30.250.17.96	Ruiz	Armando	04074	20101101	3:11:14	7234501
30.250.17.96	Clark	Michelle	04074	20101109	23:29:09	7234501
30.250.17.96	Hughen	Andrew	04072	20101118	22:18:57	7234501
30.250.17.97	Brown	Mary	04072	20101107	22:01:11	7234501
30.250.17.97	Buswell	Pamela	04074	20101130	18:15:07	7234501
30.250.17.97	Norton	Shawn	04074	20101219	6:06:17	7234501
30.250.17.97	Willis	Ramoe	04072	20101222	1:55:59	7234501
30.250.17.97	Gamage	Joe	04072	20101223	13:24:35	7234501
30.250.17.97	Lester	William	04072	20101228	18:11:22	7234501
30.250.17.98	Groton	David	04072	20101230	5:15:30	7234501
30.250.17.99	O'Donnell	David	04072	20101010	9:32:45	7234501
30.250.17.99	Maxwell	Raymond	04072	20101225	1:16:45	7234501
30.250.17.99	McNutt	Amy	04073	20101231	11:25:02	7234501
--	--	--	--	--	--	--
--	--	--	--	--	--	--
--	--	--	--	--	--	--
--	--	--	--	--	--	--

Figure 7: IPAR Address Report

From the outline of the data represented here, it is critical that the data be sent from the ISP in the correct format and order. For the larger ISPs, this extract can be programmed as an automated forwarding of data from the same systems that provide the IP address to the subscriber or from the tools that house this information for customer support troubleshooting.

For the smaller ISPs however, with less sophisticated systems, automation of this data submission may not be possible. As such, there must be a manual submission process available for providers to manually enter data into the IPAR. This manual entry would have to contain the same information and follow the same data string as shown above. Here is how the manual entry process would work.

Regardless of the size of the provider each registrant is presented with an IPAR login screen as shown here. This is the same login entry point that was shown previously, as the same portal is used whether retrieving or submitting data.

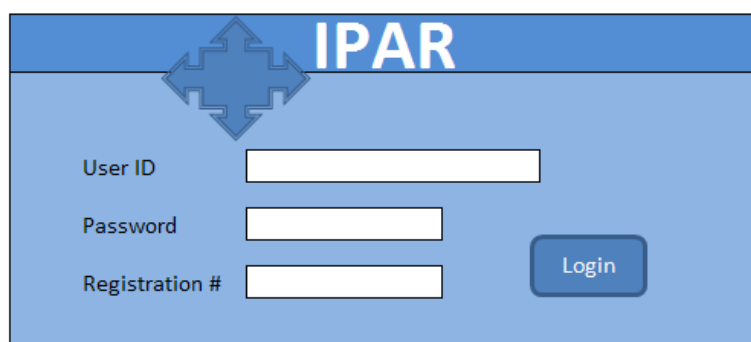
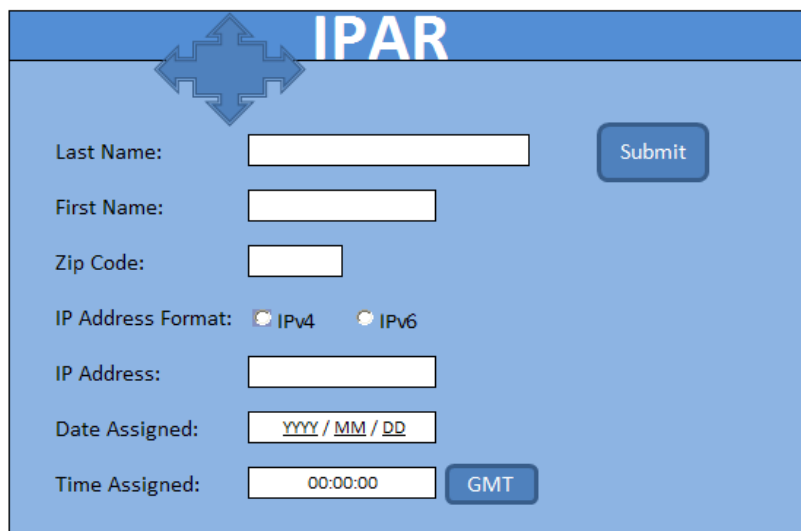
The image shows a login screen for IPAR. At the top, there is a blue header with a white logo consisting of four arrows pointing outwards from a central point, and the text "IPAR" in white. Below the header, the background is a light blue color. On the left side, there are three labels: "User ID", "Password", and "Registration #". To the right of each label is a white rectangular input field. To the right of the "Registration #" field is a blue button with the word "Login" in white text.

Figure 8: IPAR Registrant Login Screen

Based upon the registration number entered in the login screen, the user is either presented with tools to query data or the forms necessary to enter data. For the service provider who is entering data, the following screen is displayed after a successful login:



The screenshot shows a web form titled "IPAR" with a blue header. The form contains the following fields and controls:

- Last Name:** A text input field with a "Submit" button to its right.
- First Name:** A text input field.
- Zip Code:** A text input field.
- IP Address Format:** Two radio buttons labeled "IPv4" and "IPv6".
- IP Address:** A text input field.
- Date Assigned:** A text input field with a placeholder "YYYY / MM / DD".
- Time Assigned:** A text input field with a placeholder "00:00:00" and a "GMT" button to its right.

Figure 9: IPAR Manual Data Entry Screen

Here the provider is presented with all the necessary input fields to complete a manual IPAR record. Each field is formatted to ensure data is entered in the proper format for the database structure. Selecting either IP version 4 or 6 enables not only population of the single digit value within the Format Field; it also enables formatting within the corresponding IP Address input field. Formatting within the Date Input Field ensures data follows the YYYY / MM / DD format and Time can be entered directly in GMT format or converted using the GMT conversion button. Once the input record is completed, pressing the Submit button enters the data into to the IPAR database.

The screenshot shows a web form titled "IPAR" with a blue header and a blue background. The form contains several input fields and a "Submit" button. The fields are: Last Name (Ouellette), First Name (Lesa), Zip Code (04093), IP Address Format (radio buttons for IPv4 and IPv6), IP Address (10.172.28.16), Date Assigned (2010 / 12 / 25), and Time Assigned (12:22:07). A red error message is displayed next to the IP Address Format field: "* Please select the address format".

Figure 10: IPAR Error Messaging Example

Error messaging within the form structure ensures all data is entered and messages displayed when there are errors or omissions.

While enabling manual entry into the IPAR ensures even the smallest of providers can comply with reporting requirements, it is not a feasible or reasonable method for data entry for mid-size or large providers whose IP data is changing constantly. The ideal solution for accurate IPAR data is automation of the transmission process.

Requestor Accounts

Having defined the application, it is important to next define the agencies that will be allowed access to the IPAR. Privacy and security are of primary importance so a definition of who will be allowed access to retrieve information from the IPAR is critical to ensuring its acceptance as

a legitimate tool. Similar to the Department of Motor Vehicle, the IPAR is intended for use by law enforcement and government agencies. Governmental agencies that have access to interception and wiretap data include⁴⁵:

- US Government Agencies, such as the United States Government itself, or any court, department or subdivision of the United States Government. The US Department of Homeland Security is also included here.
- State Agencies. These include any state government itself, such as the State of New York, and any court, department, or subdivision of that state. Many states also define School Districts and School Administrative Units as state agencies.⁴⁶
- Public law enforcement agencies. This group includes:
 - State and Federal Attorneys General
 - State and Federal Bureaus of Investigation
 - State Troopers and Highway Patrol agencies
 - State and Federal Departments of Public Safety
 - State and Federal Bureau of Securities and Investigative Services
 - State local and municipal law enforcement departments
- Special districts. These can sometimes includes county service areas, such as taxing or zoning agencies, but only ones that qualify by providing proof that they are indeed

⁴⁵ California Department of Motor Vehicles. "Government Requester Accounts." <http://www.dmv.ca.gov/otherser/gra/govreq.htm> (accessed December 19, 2010).

⁴⁶ States and Education – State Administrative Services in Education. <http://education.stateuniversity.com/pages/2449/States-Education-STATE-ADMINISTRATIVE-SERVICES-IN-EDUCATION.html> (accessed December 28, 2010).

classified as governmental agencies. Special districts are further defined as performing proprietary functions for the state or federal government within certain limited boundaries⁴⁷, such as “New England”.

Each of these agencies, defined as ‘Government Requesters’, would be provided access to the IPAR. Many of these Federal agencies are already awarded access to surveillance data under the intercept requirements. All of these entities are granted access to criminal and public data such as motor vehicle and licensing records. Expanding access to the IPAR for these groups is well within scope of their responsibilities.

Who would not be granted access to the IPAR? Groups that are currently not defined as Governmental agencies include:

- Non-Profits Agencies regardless of whether they are fully or partially funded by another governmental agency.
- Private Police Departments. This includes any fire or police department that is fully owned and operated by a private company. These are not considered public service providers and are therefore not granted access to governmental databases.
- Sovereign or foreign nations. This includes tribal nations within the United States or foreign nations outside the United States such as Canada and Mexico. While it is common for Federal Agencies to share information with Canadian and Mexican authorities, in particular in criminal investigations that cross national borders, these

⁴⁷ University of Kansas. Center for Teaching Excellence. “Special Districts.” www.cte.ku.edu/.../Presentation%20Example%204%20Special%20Districts.ppt (accessed December 28, 2010).

foreign authorities are not awarded direct access to information on American citizens.

As such, these entities would also not be granted access to the IPAR.


Requesting access to the IPAR requires a registration process for access. While online applications are commonplace, most state agencies require completion of written forms in order to obtain access to databases such as motor vehicle registrations. One example from the State of California requires the completion of a four-page application in addition to signed agreement to a two-page Information Security Statement.⁴⁸ Other states define requirements for annual renewal and annual recertification. Areas that remain consistent in the application process include:

- Definition of the agency requesting access
- Classification of the application as New, Change, or Renewal of access
- Jurisdiction of the agency as State, Federal, or Other forms of agency
- Format of data access such as online, paper/hardcopy, tape, or secure transfer such as FTP
- Security guidelines outlining definitions of appropriate of use, security provisions, and processes for security or data breach.

These guidelines provide a sufficiently secure method of providing law enforcement and governmental agencies access to the IPAR. The data contained within the IPAR and the security considerations relative to that data fall well in line with defined guidelines for other secure

⁴⁸ State of California Department of Motor Vehicle. "Information Security Statement." <http://www.dmv.ca.gov/forms/inf/inf1128.pdf> (accessed December 28, 2010).

state and federal databases as defined above. As such, the registration process for the IPAR would follow suit. An example Requester Account Application is shown here:



Requester Account Registration Application New Change Renewal

Agency Information

Name of Agency _____

Name and Title of Agency Contact	Telephone	Email Address
----------------------------------	-----------	---------------

Agency Physical Address	City	State	County
-------------------------	------	-------	--------

Mailing Address or Same _____

Type of Agency

Federal State City
 County Special District

State or Federal Applicant

Attorney General Bureaus of Investigation Department of Public Safety
 Law Enforcement Agency * State Trooper * Highway Patrol *

* Name and Jurisdiction of Law Enforcement Entity: _____

Method of Access

Online File Transfer Paper copy
 Tape Other Specify: _____

Security Statement

By signing this form, the undersigned represents that he/she has read, understands, and agrees to the following Information Security Statement and both realizes and accepts the penalties for non-compliance to its terms:

1. I may access IPAR information only when necessary to accomplish the responsibilities of my employment and/or my agency. I may not access or use the information in the IPAR for personal reasons.
2. Inappropriate access or misuse of the IPAR includes, but is not limited to: making personal inquiries or processing transactions that contain my own records or records of my direct agency, friends, or relatives; or accessing information for any reason that is not related to my specific job responsibilities.
3. I may disclose IPAR information only to individuals who have been authorized to receive it through appropriate IPAR requester security authorization processes. In the case of disclosure of confidential IPAR information, a proper accounting of all disclosures must be made and the subject must be notified of any unauthorized disclosures.
4. I must take reasonable precautions to maintain the secrecy of any IPAR security IDs, passwords, and registration numbers provided. Reasonable precautions include, but are not limited to, not telling or allowing others to view my password or registration number; securing terminals with a locking device; storing IPAR report data in a secure place or otherwise properly destroying sensitive data; destroying data in a manner that cannot be reproduced; and reporting suspicious circumstances or unauthorized individuals that may compromise IPAR confidential data.
5. I will provide prompt notification of any indication of misuse or unauthorized use or disclosure of information obtained from the IPAR.

I certify under penalty of perjury, that I have read and understand the security policies stated above. I understand that failure to comply with these policies and regulations may result in fines and/or disciplinary or legal action in accordance with state and federal laws and regulations.

Signature	Date
-----------	------

Printed Name	Title	City	County
--------------	-------	------	--------


Figure 11: IPAR Requester Account Application

In the format displayed above, this application contains the same sections as are defined in accessing secure data from the motor vehicle database, including specifics for maintaining proper safety once access is granted. When the application process is completed and access is approved, the requester is returned an approval authorization along with their registration number and temporary credentials to use. An example authorization form is displayed here:

IPAR Access Authorization	
www.ipar.gov/NewYork	
User ID	Louellette13
Temporary Password	HY765B75RWG
Registration ID #	4869952
State	New York
<i>Registrants will be prompted to create a new permanent password upon successful login.</i>	
<i>For access issues or password assistance please contact 888-867-5309</i>	

Figure 12: IPAR Authorization Form

The descriptions above outline the process for gaining inquiry access to the IPAR database. Service providers must also complete an authorization process in order to submit data to the repository. The application and authorizations for submitters vary from those requesting inquiry. An example is shown on the following pages and includes fields for serving area, IP address assignment ranges, and types of service provided.



Provider Submission Account Registration Application New Change Renewal

Service Provider Information

Name of Service Provider EID Number:

Name and Title of Service Provider Contact Telephone Email Address

Physical Address City State County

Mailing Address or Same

Type of Internet Services Provided check all that apply

ISDN T1 Cable modem
 DSL Dial-Up / Analog Modem Wireless

Service Area:

Municipal State _____ Multiple States *

* If multiple states, specify states of operation: _____

Method of Submission

Electronic Manual Both

Security Statement

By signing this form, the undersigned represents that he/she has read, understands, and agrees to the following Information Security Statement and both realizes and accepts the penalties for non-compliance to its terms:

- As a representative of the service provider listed above, I may access the IPAR only for the purposes of submitting address assignment data and only when necessary to accomplish the responsibilities as a service provider or agent thereof. I will not request query access to information in the IPAR whether for business or personal reasons.
- Inappropriate access or misuse of the IPAR includes, but is not limited to: submitting or processing transactions that contain my own records or records of my direct agency, friends, or relatives unless these are served by the providing entity and processed electronically as part of the automatic submission process; or falsely submitting erroneous or intentionally altered information to the IPAR for any reason.
- As a representative of the service provider listed above, I may disclose IPAR site and/or access information only to individuals who have been authorized to receive it through appropriate IPAR submitter security authorization processes. In the case of disclosure of confidential IPAR information, a proper accounting of all disclosures must be made and the subject(s) must be notified of any unauthorized disclosures.
- As a representative of the service provider listed above, I must take reasonable precautions to maintain the secrecy of any IPAR security IDs, passwords, and registration numbers provided. Reasonable precautions include, but are not limited to, not telling or allowing others to view password or registration number; securing terminals with a locking device; storing IPAR submission data in a secure electronic and encrypted format that is restricted from access; and reporting suspicious circumstances or unauthorized individuals that may compromise IPAR submission data.
- As a representative of the service provider listed above I will provide prompt notification of any indication of misuse or unauthorized use or disclosure of information obtained from the IPAR.

As a representative of the service provider listed above I certify under penalty of perjury, that I have read and understand the security policies stated above. I understand that failure to comply with these policies and regulations may result in fines and/or disciplinary or legal action in accordance with state and federal laws and regulations.

Signature Date

Printed Name Title City County

Figure 13: IPAR Provider Submission Account Registration Application Page 1

IPAR Submission Access Authorization	
www.ipar.gov/Vermont	
User ID	Coxcable115
Password	PK656C84STH
Registration ID #	1978061
Submission Site:	ftp://10.198.62.35:34
State	Vermont
<i>Retain this information for automated submission to the IPAR system. For manual submission entry go to:</i>	
www.ipar.gov/Vermont/OnlineEntry	
<i>For access issues or password assistance please contact 888-867-5309</i>	

Figure 14: IPAR Service Provider Submission Access Authorization Form

This application and approval process follows similar guidelines and processes in use with the Department of Motor Vehicles. While much of the process has migrated to online access and electronic entry, a great deal of the application and authorization processes remain paper based. In contacting the local state agency to determine why much of the application process is still document-based, the following reasoning was provided⁴⁹:

- Certain systems did not support automation for these processes
- Age of the system and / or application didn't support online entry or access (no front-end application entry point exists)
- State funding at this time did not support the capital needed to fully automate the application and authorization process

⁴⁹ Curtis, Kathleen. Phone interview. Kathleen Curtis, Bureau of Motor Vehicles, State of Maine. (Oct. 7, 2010).

- Preference within certain legal and state departments were for a handwritten signature to be present on the application documentation, where automation of access did not allow for handwritten signatures
- Belief that the physical copy and written application process provided greater security control than allowing open online access (no ability to confirm the validity of the user requesting access)

There is legitimacy to the points referenced above in that many state systems are aged and may not support many of the upgrades needed for online access. State governments are also short on funding and would find it financially difficult to retro fit applications to support fully automated registration and authorization. How, then, do we fund the creation of the IPAR?

Who pays?

Regardless of which entity manages the data, it is ultimately the consumer who has to pay for it. The growing costs of data archiving and management for an ISP, in the millions of dollars per year, is eventually transferred on to the subscriber as part of the ISP's cost of doing business.

The IPAR solution decreases the archiving aspect for an ISP, which reduces both onsite disk and offsite storage costs, however the systems that regulate usage and allocation of IP addressing for subscribers would continue to be managed by the provider. This means only a portion of the costs of IP address management are shifted away from the ISP.

On the receiving end, State and Federal agencies would now bear the costs of storage and archiving of the IPAR. While this adds to the initial cost of storage hardware and offsite record retention, there are several significant cost and operational improvements that offset the expense.

- Reimbursement for subpoena processing costs. There can be significant costs involved in the request, processing, and serving of an official subpoena requesting IP information. An IPAR solution removes at least one subpoena, in a two-step subpoena process, the one to the ISP to determine the user of an IP address. ISPs are granted the ability to charge for their services in response to subpoena requests for information. An example of cost reimbursement fees for Cox Communication is included in *Addendum A*. Fees can include costs for basic information, expedited handling, additional per-IP fee, copying fees, excessive account lookup fees, data media fees, and incorrect ISP fees⁵⁰. Costs charged to the law enforcement agencies ultimately become a cost of the state or governmental agency they are funded through.
- Costs for law enforcement. When law enforcement identifies an activity that warrants investigation, they must first make a request to the District Attorney's office for a subpoena to be issued. A typical DA's office holds a backlog of subpoena requests, so there is a usual delay in the initial turnaround time for the request to be processed. Once the subpoena is submitted to the ISP, there is a normal response window of

⁵⁰ Cox Communication, Inc. "Cox Communication LEA Information Policy", last modified October 1, 2009. *Notice to parties serving subpoenas on Cox Communication*. <http://cryptome.org/isp-spy/cox-spy.pdf> (accessed October 1, 2010).

anywhere from 10 days to up to 30 days to provide the response. If this is part one of a two-step subpoena, then the process repeats when the first response is returned. In these scenarios, it is not unusual for a request by law enforcement for IP information to take two months and longer. The delays mean increased cost for law enforcement as investigations take longer and criminal activity continues without impedance. This also means increased costs for states that fund the expenses of the state's District Attorney's offices. With IP address information stored in an IPAR, there is a direct reduction in state costs both at the district attorney and law enforcement levels.

- Witness costs. Depending on the jurisdiction, State and/or Federal governments cover the cost of ISP witnesses that are subpoenaed to testify in criminal cases. Costs can include the cost of travel, time, records submission and others. In a criminal case, the government covers all costs of the prosecution. With direct access to data from the IPAR, these ISP witness expenses are reduced or removed.
- Small providers. Certain small ISPs have been unable to comply with current data retention policies. They have not had either the infrastructure or the financial ability to record and store subscriber IP assignments. Building such an infrastructure is cost prohibitive based on their smaller revenue streams, leaving them sandwiched between the costs to comply and the penalties of noncompliance. An IPAR alternative would allow these small suppliers to provide subscriber information, whether manually or automated, to the IPAR and reduce the expense burden of compliance. This would also

provide subscriber information for a subset of customers where once this information was unobtainable.

- Taxation loses from copyright infringement. In a study conducted by The Institute for Policy Innovation, titled "The True Cost of Copyright Industry Piracy to the U.S. Economy," the report found that copyright infringement "costs the U.S. economy \$58.0 billion in total output, costs American workers 373,375 jobs and \$16.3 billion in earnings, and costs federal, state, and local governments \$2.6 billion in tax revenue."⁵¹ The key components for reducing piracy comes in improved policing and more rapid identification of offenders. An IPAR solution allows law enforcement more streamlined and more real-time access to user identification, greatly improving the chances of catching perpetrators. At a minimum, a 1% improvement in identification equates to \$2.6 million in increased tax revenues. With accessibility to up-to-date IP address information, an IPAR solution is likely to provide substantial improvements to tax revenues far in excess of 1% thus far in excess of \$2.6 million.

Considering the costs outlined above, the IPAR is more than a simple transference of process and fees from one entity to another. There are true costs savings to be realized in a more streamlined, centralized repository. While these are a few of the cost reductions, there are also certain fees and taxes that offset the costs of an IPAR. Telecommunications companies are required to assess State and local taxes for the services they provide to their customers. Those

⁵¹ Photo Attorney®. "The Cost of Copyright Infringement." <http://www.photoattorney.com/2007/10/costs-of-copyright-infringement.html> (accessed October 3, 2010).

taxes would continue to be assessed and paid to the state. Service providers must also assess and collect Universal Service Fees, as well as FCC fees and 911 fees.⁵² These fees have been developed over time to assist with cost allocation for services such as emergency fire and rescue, as well as costs of delivering services to rural areas. If ISPs were assessed a .5% fee for each internet subscriber, and an average consumer brings \$45/month in revenues per internet account, the IPAR fee would amount to a 22.5 cent per month cost per subscriber. While this would help with the reallocation of the data archiving costs for state and federal agencies, the corresponding reduction in staffing and data management for the ISP would far outweigh the monthly IPAR fee.

ISPs can also be charged for ISPID registration. As outlined above, the registration process for the IPAR provides the ISPID tag to be associated with each incoming IP address record. In addition, the ISP is given a specific and secure IP address to be used as a secure tunnel through the firewalls to transmit update records to the database. Costs for registration would be minimized to encourage even the smaller providers to participate, however even the smaller fee would help offset the costs involved in the creation and securing of the dedicated IP tunnel per ISP.

As outlined previously, third party providers could also provide a method of offsetting some of the IPAR costs. Third parties offer a variety of legal and integration services such as completion of court-ordered records, data communication interception services, and data retention and archiving services. In addition to providing these critical services to ISPs, these same services

⁵² Federal Communications Commission. "Understanding your Telephone Bill." *FCC Consumer Facts*. <http://www.fcc.gov/cgb/consumerfacts/understanding.html> (accessed October 30, 2010).

could be used by state and federal agencies as a method to reduce systems development and corresponding support staff. These are companies that have already met the stringent guidelines for governmental approval relative to security, privacy, and confidentiality thus many of the systems could be provided by outsourced entities at less cost.

Finally, referencing back to the Department of Motor Vehicle model, other charges could also apply for accessing data in the IPAR. One example in use with the DMV is the fee assessed to obtain a copy of one's own records.⁵³ It is common for individuals to want to obtain their own motor vehicle records whether it is for an open legal case or for purposes of verifying the data contained within the records. This would also be a reasonable request of internet subscribers or for legal teams representing these subscribers. Where the data applies to the specific customer, the question of privacy does not factor in and the records can be provided (upon confirmation of the subscriber's information) with a small fee assessed to offset the cost of producing the records. Other fees apply if records are requested via tape, FTP, online or other electronic methods. While individually each of these fees is small, collectively these revenues can provide a reasonable offset to some of the systems and storage costs that will come along with an IPAR deployment.

⁵³ Department of Driver Services. "How do I request a driver history report (MVR)?" December 13, 2010. <http://www.dds.ga.gov/drivers/DLdata.aspx?con=1740840381&ty=dl> (accessed December 28, 2010).

Future Development and Expansion

The future for IPAR lies in the opportunities this type of database would offer in integration with other databases and other services. While protecting the privacy of IP address information is key, providing consolidated data to those agencies that already have access to the private information is an intriguing future for the IPAR. Use of the internet has become the norm. With more and more applications becoming web-enabled or internet served, the use of IP addressing will also become the norm across many more devices and services. Is it possible that vehicles could be assigned IP addresses for their built in navigation and emergency systems? The answer is yes. That reality is not in the future but one that exists now, in vehicles like the Chevy Volt. According to GM, "Each Volt also has its own IP address..." based on a partnership with IBM and GM and integrating 10 million lines of software code into the new car.⁵⁴ Could this imply a future where the DMV and the IPAR are integrated into one database where each vehicle's registration also includes their IP address?

Other integration options also exist. With a fully functioning IPAR, integrating IP address data to a criminal background database becomes possible. Marrying these two systems could provide enormous benefits to law enforcement in tracking criminal behavior beyond physical activity to combine it with real-time and historical online activity. This becomes more compelling if the vehicle registration database evolves to include in-car IP addresses as referenced above, and now all of these separate entities are combined into one consolidated

⁵⁴ Racoma, J. Angelo. November 3, 2010. "Chevy Volt Electric Cars Each Have Their Own IP Addrss." *IBM & GM Say Volt's Electronic Control Unit has 10M Lines of Code & Own IP Address*. <http://nexus404.com/Blog/2010/11/03/chevy-volt-electric-cars-each-have-their-own-ip-address-ibm-gm-say-volts-electronic-control-unit-has-10m-lines-of-code-own-ip-address/> (accessed December 27, 2010).

and complete system. Motor vehicle records and vehicular offenses could be included and linked by the IP addresses assigned to each new vehicle. Similar to the ability to track suspended or revoked licenses, could this integrated data be used to track suspended or revoked user IP addresses?

Some of this integration exists today. A user's online criminal activity, such as child pornography, becomes part of their criminal record. Could the reverse be true and a person's physical criminal activity be used to identify, and perhaps also prohibit, online activity? This is a much more compelling and more easily achievable concept if systems such as these are integrated.

Continuing on with the concept of integration, let's consider other state and federal systems that are utilized for employment background checks. This information is important to potential employers to determine validity of criminal information on an application as well as to confirm driving eligibility in the event the perspective employee would have access to company vehicles. Could a system like the IPAR eventually be integrated into a background check report? If so, then the combined systems could provide information on a user's IP history and potentially any suspension or revocation of online access. This could be important information to a business that needs to ensure information is safeguarded and online behavior is appropriate with business practices. This also leads to interesting concerns relative to user confidentiality and privacy, and the separation of personal and workplace internet usage activity.

Conclusion

This thesis analyzes the process of IP assignment and internet policing and outlines that a national IP address database will allow law enforcement and governmental agencies improvements in real-time, secure access to subscriber identifying information without compromising the security and privacy of internet users. The present process for IP Address allocation, retention, and protection is no longer sufficient to support retention periods, archiving costs, and privacy protection. The improvements outlined in the implementation of a centralized IP address database support recording and archiving of IP Address information, in a method that is more cost effective, more efficient, and more secure than the current model. Furthermore, establishing a foundation for this system that is based on existing systems and existing processes encourages support for this new concept and reduces concerns from the perspective of user privacy and safety. American citizens think nothing of affixing a license plate to their vehicles to allow them use of the nation's highways. This is a simple analogy to enable a similar treatment for an IP address, in a manner that citizens understand and have an established confidence that their information is protected for use only by the enforcement agencies that need it. Thirty years after the true inception of IP version 4, it is no longer feasible or reasonable to continue following legislative and operational guidelines that were established long before the Internet was a household or handheld service. The centralized IP address database provides an improved and secure method to better support the new all-IP technological environment of the present day and well into the future.

Addendum A

Cox rate sheet for subpoena processing

RECORDS CUSTODIAN INFORMATION FOR COX COMMUNICATIONS		As of 9/1/2009																																							
See also: http://www.cox.com/policy/tainformation/default.asp or call (404) 269-0100 Cox Privacy Notice: http://www.cox.com/policy/annualprivacynotice.asp																																									
SubpoenaResponse@cox.com Fax: (404) 269-1898																																									
<p>Service of Process - Cox Communications and its subsidiaries accept service of subpoenas, warrants and court orders, subject to payment of costs, by email at SubpoenaResponse@cox.com or by fax at (404) 269-1898. <u>We do not accept service at any of our local offices.</u> Our physical address is Records Custodian, Cox Communications, 1400 Lake Hearn Drive, Atlanta, GA 30319-1464. Physical service may be made on the agent for service of process for Cox Communications, available from the Secretary of State wherever we do business or on Corporation Service Company, 40 Technology Parkway South, Suite 400, Norcross, GA 30092.</p>																																									
<p>Restrictions - Acceptance of service by facsimile or email is strictly conditioned upon payment of charges. Cox reserves the right to require payment in advance, to withhold delivery until payment and to seek enforcement of charges, including cost of collection. Entities that fail to pay charges must serve process upon the registered agent for Cox Communications within the appropriate state and requests for expedited response will not be granted. You will be notified if hourly charges apply and can request an estimate.</p>																																									
<p>Response Time - Requests are handled in the order received, subject to pending expedited requests. <u>Responsive information is generally provided within 10 business days.</u> Expedited response for information other than call records, if available resources permit, will generally be provided within 3 business days. Extensive toll and call record detail requests may require 30 days or more.</p>																																									
<p>Questions - During business hours Eastern Time, all questions should be directed as follows:</p> <ul style="list-style-type: none"> • Fax: (404) 269-1898 • Email: SubpoenaResponse@cox.com • Phone (404) 269-0100 (Voice messages will be returned within 1 business day) 																																									
<p>Status Requests - <u>For security reasons, all questions must be submitted in writing along with a copy of the subpoena and response.</u> To prevent delays in response to your request and those of others, please do not ask for the status of a request prior to 10 business days for subscriber information, 3 days for expedited requests and 30 days for call records. You may then fax a copy of your original subpoena with a cover page asking for the status.</p>																																									
<p>Records Retention - The following retention policies generally apply to frequently sought records:</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 80%;">IP Assignment Logs</td> <td>Up to 6 months</td> </tr> <tr> <td>Subscriber Information</td> <td>3 years</td> </tr> <tr> <td>Call Records</td> <td>18 months (up to 36 in certain states)</td> </tr> <tr> <td>LEA Preservation Requests</td> <td>90 days (additional 90 days upon further request)</td> </tr> </table>			IP Assignment Logs	Up to 6 months	Subscriber Information	3 years	Call Records	18 months (up to 36 in certain states)	LEA Preservation Requests	90 days (additional 90 days upon further request)																															
IP Assignment Logs	Up to 6 months																																								
Subscriber Information	3 years																																								
Call Records	18 months (up to 36 in certain states)																																								
LEA Preservation Requests	90 days (additional 90 days upon further request)																																								
<p>Requirement for Court Order or Warrant - Except as provided in 18 USC 2703, content of communications may not be provided without court order or warrant.</p>																																									
<p>Cost Reimbursement (18 U.S.C. § 2706)</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30px;"><input type="checkbox"/></td> <td style="width: 200px;">\$40.00</td> <td>Per account for basic information *</td> </tr> <tr> <td><input type="checkbox"/></td> <td>\$80.00</td> <td>Per account for expedited handling</td> </tr> <tr> <td><input type="checkbox"/></td> <td>\$40.00/Month</td> <td>Telephone <u>call detail</u> records (other than toll)</td> </tr> <tr> <td><input type="checkbox"/></td> <td>No Charge</td> <td>Telephone <u>toll record</u> and Cox telephone subscriber records of 10 or less**</td> </tr> <tr> <td><input type="checkbox"/></td> <td>\$5.00/Account</td> <td>In excess of 10 subscribers</td> </tr> <tr> <td><input type="checkbox"/></td> <td>\$0.25/Page</td> <td>Photocopies and facsimiles exceeding 10 pages</td> </tr> <tr> <td><input type="checkbox"/></td> <td>\$25.00</td> <td>Data on CD-ROM</td> </tr> <tr> <td><input type="checkbox"/></td> <td>\$25.00</td> <td>Express delivery</td> </tr> <tr> <td><input type="checkbox"/></td> <td>\$75.00/Hr./Staff</td> <td>Requests requiring greater than 0.5 hours (\$40.00 minimum)</td> </tr> <tr> <td><input type="checkbox"/></td> <td>\$80.00 plus \$150.00Hr./Staff</td> <td>For preservation or expedited handling, if available</td> </tr> <tr> <td><input type="checkbox"/></td> <td>No Charge</td> <td>Non-expedited child pornography or endangerment investigations and investigations of harassing or abusive calls, if documented when requested and unless expedited response is sought</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Pen Register/Trap and Trace</td> <td>\$2500 for 60 days - \$2000 for each additional 60 days</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Wiretap</td> <td>\$3500 for 30 days - \$2500 for each additional 30 days</td> </tr> </table> <p>*Requests based on IP addresses <u>must</u> include date, time and time zone information in order to receive a response. ** Telephone subscriber requests from law enforcement in excess of 10 accounts or otherwise voluminous are subject to charge under 18 USC 2706. Inaccurate requests concerning non-Cox subscribers require a fee of \$25 per non-Cox request. Law enforcement can determine providers at http://www.npac.com. Telephone account information in civil matters is charged at \$40 per account.</p>			<input type="checkbox"/>	\$40.00	Per account for basic information *	<input type="checkbox"/>	\$80.00	Per account for expedited handling	<input type="checkbox"/>	\$40.00/Month	Telephone <u>call detail</u> records (other than toll)	<input type="checkbox"/>	No Charge	Telephone <u>toll record</u> and Cox telephone subscriber records of 10 or less**	<input type="checkbox"/>	\$5.00/Account	In excess of 10 subscribers	<input type="checkbox"/>	\$0.25/Page	Photocopies and facsimiles exceeding 10 pages	<input type="checkbox"/>	\$25.00	Data on CD-ROM	<input type="checkbox"/>	\$25.00	Express delivery	<input type="checkbox"/>	\$75.00/Hr./Staff	Requests requiring greater than 0.5 hours (\$40.00 minimum)	<input type="checkbox"/>	\$80.00 plus \$150.00Hr./Staff	For preservation or expedited handling, if available	<input type="checkbox"/>	No Charge	Non-expedited child pornography or endangerment investigations and investigations of harassing or abusive calls, if documented when requested and unless expedited response is sought	<input type="checkbox"/>	Pen Register/Trap and Trace	\$2500 for 60 days - \$2000 for each additional 60 days	<input type="checkbox"/>	Wiretap	\$3500 for 30 days - \$2500 for each additional 30 days
<input type="checkbox"/>	\$40.00	Per account for basic information *																																							
<input type="checkbox"/>	\$80.00	Per account for expedited handling																																							
<input type="checkbox"/>	\$40.00/Month	Telephone <u>call detail</u> records (other than toll)																																							
<input type="checkbox"/>	No Charge	Telephone <u>toll record</u> and Cox telephone subscriber records of 10 or less**																																							
<input type="checkbox"/>	\$5.00/Account	In excess of 10 subscribers																																							
<input type="checkbox"/>	\$0.25/Page	Photocopies and facsimiles exceeding 10 pages																																							
<input type="checkbox"/>	\$25.00	Data on CD-ROM																																							
<input type="checkbox"/>	\$25.00	Express delivery																																							
<input type="checkbox"/>	\$75.00/Hr./Staff	Requests requiring greater than 0.5 hours (\$40.00 minimum)																																							
<input type="checkbox"/>	\$80.00 plus \$150.00Hr./Staff	For preservation or expedited handling, if available																																							
<input type="checkbox"/>	No Charge	Non-expedited child pornography or endangerment investigations and investigations of harassing or abusive calls, if documented when requested and unless expedited response is sought																																							
<input type="checkbox"/>	Pen Register/Trap and Trace	\$2500 for 60 days - \$2000 for each additional 60 days																																							
<input type="checkbox"/>	Wiretap	\$3500 for 30 days - \$2500 for each additional 30 days																																							
<p>Payment Methods: <u>Include invoice reference number</u> with payment. American Express, Visa and MasterCard accepted.</p>																																									
Check:	Make payable to Cox Communications, Inc. (Tax ID # 58-2112281) (Dun's # 789111374-1234) Subpoena Compliance Payments Cox Communications 1400 Lake Hearn Drive Atlanta, GA 30319-1464																																								
EFT:	Contact us for instructions																																								
<p>Contact Information - (Please do <u>not</u> direct status requests or questions concerning subpoenas to these individuals.)</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 40%;">Saguonna Riley</td> <td style="width: 30%;">saguonna.riley@cox.com</td> <td style="width: 30%;">Phone: (404) 269-6841</td> </tr> <tr> <td>Randy Cadenhead, Esq.</td> <td>randy.cadenhead@cox.com</td> <td>Phone: (404) 269-6761</td> </tr> <tr> <td>Bob Brand (National Security/Classified - 24/7)</td> <td>Phone: (678) 645-0670</td> <td>Fax - (678) 645-1679</td> </tr> <tr> <td colspan="3">After Business Hours - Emergency Only (Eastern Time) 1 (877) 866-4474</td> </tr> </table>			Saguonna Riley	saguonna.riley@cox.com	Phone: (404) 269-6841	Randy Cadenhead, Esq.	randy.cadenhead@cox.com	Phone: (404) 269-6761	Bob Brand (National Security/Classified - 24/7)	Phone: (678) 645-0670	Fax - (678) 645-1679	After Business Hours - Emergency Only (Eastern Time) 1 (877) 866-4474																													
Saguonna Riley	saguonna.riley@cox.com	Phone: (404) 269-6841																																							
Randy Cadenhead, Esq.	randy.cadenhead@cox.com	Phone: (404) 269-6761																																							
Bob Brand (National Security/Classified - 24/7)	Phone: (678) 645-0670	Fax - (678) 645-1679																																							
After Business Hours - Emergency Only (Eastern Time) 1 (877) 866-4474																																									

Addendum B – 2009 Comcast Customer Privacy Notice

2009 Comcast Customer Privacy Notice

For Cable Television, High-Speed Internet, and Phone Services

Why is Comcast providing this notice to me?

As a subscriber to cable service or other services provided by Comcast, you are entitled under Section 631 of the federal Cable Communications Policy Act of 1984, as amended, (the "Cable Act") to know the following:

- the limitations imposed by the Cable Act upon cable operators in the collection and disclosure of personally identifiable information about subscribers;
- the nature of personally identifiable information we collect;
- the nature of the use of personally identifiable information;
- under what conditions and circumstances we may disclose personally identifiable information and to whom;
- the period during which we maintain personally identifiable information;
- the times and place at which you may have access to your personally identifiable information; and
- your rights under the Cable Act concerning personally identifiable information and its collection and disclosure.

Personally identifiable information is information that identifies a particular person; it does not include aggregate data that does not identify a particular person or persons. This notice is also provided to you in accordance with applicable California law, which only applies to our customers located in California who are served by a cable television corporation.

In addition, Section 702 of the federal Telecommunications Act of 1996, as amended, (the "Telecommunications Act") provides additional privacy protections for certain information related to our phone services:

- information about the quantity, technical configuration, type, destination, location, and amount of your use of the phone services; and
- information contained on your telephone bill concerning the phone services you receive.

That phone information, when matched to your name, address, and telephone number is known as customer proprietary network information or CPNI for short. This notice, which includes our CPNI Policy, describes what CPNI information we obtain, how we protect it, and how it may be used. If you are a customer of our phone services, you have the right, and Comcast has a duty, under the Telecommunications Act, to protect the confidentiality of CPNI. We will also honor any restrictions applied by state law, to the extent applicable. **WE EXPLAIN BELOW UNDER "HOW DO I GIVE OR WITHHOLD MY APPROVAL FOR COMCAST TO USE CPNI TO MARKET ADDITIONAL PRODUCTS AND SERVICES TO ME?" HOW YOU CAN APPROVE OUR USE OF CPNI OR WITHDRAW YOUR APPROVAL.**

Special Note: Our CPNI Policy applies to the communications-related services provided by Comcast Business Communications, Comcast Digital Phone, Comcast Digital Voice, and Comcast Long Distance.

In this notice, the terms "Comcast," "we," "us," or "our" refer to the operating company subsidiary or subsidiaries of Comcast Corporation that (i) owns and/or operates the cable television system in your area pursuant to a cable television franchise with the local franchising authority, or (ii) is operating in your area as Comcast Business Communications, Comcast Digital Phone, Comcast Long Distance, or Comcast Digital Voice. The term "you" refers to you as a subscriber to one or more of our cable service and other services.

I. Collection

What kind of information does this notice apply to?

The Cable Act applies to personally identifiable information that you have furnished to Comcast, or that Comcast has collected using the cable system, in connection with the provision of cable service or other services. The Telecommunications Act applies to CPNI related to our regulated phone services, and certain orders of the Federal Communications Commission apply the CPNI rules to our

interconnected voice over Internet protocol communications services. This notice applies to our cable television service, our high-speed Internet service, and our phone services as provided for by applicable law and except as otherwise noted.

Special Note: This notice only covers information that is collected by Comcast in connection with the provision of our cable television service, our high-speed Internet service, and our phone services to you as a subscriber to one or more of these services. It does not cover information that may be collected through any other products, services, or websites, even if accessed through our services and even if co-branded with them. You should read the privacy policies for these other products, services, and websites to learn how they handle your personal information.

For what purposes may Comcast collect personally identifiable information and CPNI?

The Cable Act authorizes Comcast as a cable operator to use the cable system to collect personally identifiable information concerning any subscriber for the following purposes:

- in order to obtain information necessary to render our cable service or other services to our subscribers; and
- to detect unauthorized reception of cable communications.

The Cable Act prohibits us from using the cable system to collect personally identifiable information concerning any subscriber for any purposes other than those listed above without the subscriber's prior written or electronic consent.

The Telecommunications Act authorizes us to use, disclose, or permit access to individually identifiable CPNI in our provision of:

- the telecommunications service from which this information is derived; or
- services necessary to, or used in, the provision of these services, including the publishing of directories.

The Telecommunications Act prohibits us from using CPNI for any purposes other than those listed above except as permitted or required by law or with your approval.

What kind of personally identifiable information and CPNI does Comcast collect?

Comcast collects information from you at several different points when you initiate and use our services. Some of this information is personally identifiable information, but much of it is not. We collect certain personally identifiable information that our subscribers furnish to us in connection with the provision of cable service or other services. In order to provide reliable, high quality service to you, we keep regular business records containing information about you that may constitute personally identifiable information. These records include some, but typically not all, of the following information:

- your name;
- service address;
- billing address;
- e-mail address;
- telephone number;
- driver's license number;
- social security number;
- bank account number;
- credit card number; and
- other similar account information.

With respect to phone services, examples of CPNI include information typically available from telephone-related details on your monthly bill, such as:

- location of service;
- technical configuration of service;

- type of service;
- quantity of service;
- amount of use of service;
- calling patterns; and
- other information contained on your bill for local and long distance services.

CPNI does not include your name, address, and telephone number, because the Telecommunications Act classifies that information as "subscriber list information" which is not subject to the protections applicable to CPNI. However, that information is also subject to certain protections as described below under "To whom may Comcast disclose personally identifiable information?"

We also collect and maintain certain other information about your account. For example, this information may include:

- billing, payment, and deposit history;
- additional service information;
- customer correspondence and communications records;
- maintenance and complaint information;
- records indicating the number of television sets, set-top boxes, modems, or telephones connected to our cable system; and
- additional information about the service options you have chosen.

Some of our services permit you to establish secondary accounts, and if you do so we collect similar information in order to establish and service the secondary accounts. During the initial provisioning of our services, and during any subsequent changes or updates to our services, Comcast may collect technical information about your televisions, any set-top boxes, computer hardware and software, cable modems, telephones, and/or other cable or other service-related devices, and customization settings and preferences. Additionally, if you rent your residence, we may have a record of whether landlord permission was required prior to installing our cable facilities as well as your landlord's name and address.

What kind of information do you collect if I use interactive or transactional services or television viewing controls?

When you use our interactive or other transactional services such as video on demand, for example, our systems may automatically collect certain information about your use of these services. Most of this information is not personally identifiable information and it is simply used, for example, to carry out a particular request you make using your remote control, set-top box, or other equipment. This may include information required to change your television channel, review listings in an electronic program guide, pause or fast forward through certain on demand programs, or invoke a calling feature, among other things. It may also include other information such as the time you actually use our services and the use of other features of our services, and which menus and menu screens are used most often and the time spent using them.

In order to carry out a particular request you make to watch a pay-per-view program or purchase a product, service, or feature, for example, our system may collect certain personally identifiable information. This information typically consists of account and billing-related information such as the pay-per-view programs or other products, services, or features ordered so that you may be properly billed for them. Follow your program guide commands or any special instructions on your video screen when you make these transactional requests. These commands and instructions will explain your choices so that you can complete or cancel your requests as you wish.

What kind of information do you collect and use to improve your cable services and deliver relevant advertising?

Our cable systems may collect anonymous and/or aggregate information using set-top boxes and other equipment. We use this information to determine which programs are most popular, how many people watch a program to its conclusion, and whether people are watching commercials, for example. As described below under "How does Comcast use personally identifiable information and CPNI?", we may provide subscriber lists or certain anonymous and/or aggregate information to third parties working on our behalf such as audience measurement or market research firms, for example. These firms may combine this information with other aggregated or non-aggregated demographic information (such as census records) to provide us with audience analysis data though we will require them to remove personally identifiable information about our subscribers from this data. We use this information to improve our cable television service and other services and make programming and advertising more relevant to our subscribers. We

may also use this information to distribute and deliver relevant programming and advertising to you without disclosing personally identifiable information about you to programmers or advertisers. In addition to this privacy notice, we may provide additional notices to you regarding specific advertising or other initiatives. These notices will describe the initiatives in greater detail and may, as appropriate, contain information you can use to choose to participate, or not participate, in these initiatives.

II. Use

How does Comcast use personally identifiable information and CPNI?

We collect, maintain, and use personally identifiable information and CPNI as permitted by the Cable Act and the Telecommunications Act and other applicable laws. We use this information primarily to conduct business activities related to providing you with our cable service and other services, and to help us detect theft of service. Generally speaking, we use personally identifiable information in connection with:

- billing and invoicing;
- administration;
- surveys;
- collection of fees and charges;
- marketing;
- service delivery and customization;
- maintenance and operations;
- technical support;
- hardware and software upgrades; and
- fraud prevention.

More specifically, we also use personally identifiable information to:

- install, configure, operate, provide, support, and maintain our cable service and other services;
- confirm you are receiving the level(s) of service requested and are properly billed;
- identify you when changes are made to your account or services;
- make you aware of new products or services that may be of interest to you;
- understand the use of, and identify improvements to, our services;
- detect unauthorized reception, use, or abuse of our services;
- determine whether there are violations of any applicable policies and terms of service;
- manage the network supporting our services;
- configure cable service and other service-related devices; and
- comply with law.

The Telecommunications Act further permits Comcast to use, disclose, and permit access to CPNI obtained from our customers, either directly or indirectly, to:

- initiate, render, bill, and collect for telecommunications services;
- protect our rights and property, and protect our users of these services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, these services;
- provide any inbound telemarketing, referral, or administrative services to you for the duration of the call, if you initiated the call and you approve of the use of this information to provide these services; and
- to provide call location information concerning the user of a commercial mobile phone service.

With respect to phone services, unless we obtain your approval in accordance with our policies described below under "How do I give or withhold my approval for Comcast to use CPNI to market additional products and services to me?" Comcast may not use CPNI to market products and services to you other than the phone services.

Comcast transmits, and may collect and store for a period of time, personally identifiable and non-personally identifiable information about you when you use our high-speed Internet and phone services to:

- send and receive e-mail, video mail, and instant messages;
- transfer and share files;
- make files accessible;
- visit websites;
- place or receive calls;
- leave and receive voice mail messages;
- use the SmartZone™ Communications Center as applicable;
- establish custom settings or preferences;
- communicate with us for support; or
- otherwise use the services and their features.

Our transmission, collection, and storage of this information is necessary to render the services. In certain situations, third-party service providers may transmit, collect, and store this information on our behalf to provide features of our services. These third parties are not permitted to use your personally identifiable information except for the purpose of providing these features.

We may also combine personally identifiable information, which we collect as described in this notice as part of our regular business records, with personally identifiable information obtained from third parties for the purpose of creating an enhanced database or business records. We may use this database and these business records in marketing and other activities related to our cable service and other services. We also maintain records of research concerning subscriber satisfaction and viewing habits, which are obtained from subscriber interviews and questionnaires.

III. Disclosure

Under what circumstances may Comcast disclose personally identifiable information to others?

Comcast considers the personally identifiable information contained in our business records to be confidential. The Cable Act authorizes Comcast as a cable operator to disclose personally identifiable information concerning any subscriber for the following purposes if the disclosure is:

- necessary to render, or conduct a legitimate business activity related to, the cable service or other services provided to the subscriber;
- required by law or legal process (described below under "When is Comcast required by law to disclose personally identifiable information and CPNI by law?"); or
- of the names and addresses of subscribers for "mailing list" or other purposes (subject to each subscriber's right to prohibit or limit this disclosure and the CPNI Policy described below under "How do I place myself on Comcast's 'do not call' and 'do not mail' lists?").

The Cable Act prohibits us from disclosing personally identifiable information concerning any subscriber for any purposes other than those listed above without the subscriber's prior written or electronic consent.

To whom may Comcast disclose personally identifiable information?

We may disclose personally identifiable information as provided for in the Cable Act when it is necessary to render, or conduct a legitimate business activity related to, the cable service or other services we provide to you. These kinds of disclosures typically involve billing and collections, administration, surveys, marketing, service delivery and customization, maintenance and operations, and fraud prevention, for example. We may also collect, use, and disclose information about you in non-personally identifiable or aggregate formats, such as ratings surveys and service usage and other statistical reports, which do not personally identify you, your particular viewing habits, or the nature of any transaction you have made over the cable system. The frequency of any disclosure of personally identifiable information varies in accordance with our business needs and activities.

The Cable Act authorizes Comcast as a cable operator to disclose limited personally identifiable information to others, such as charities, marketing organizations, or other businesses, for cable or non-cable "mailing list" or other purposes. From time to time we may disclose your name and address for these purposes. However, you have the right to prohibit or limit this kind of disclosure by contacting us by telephone at 1-800-COMCAST or by sending us a written request as described below under "How do I contact Comcast?" Any "mailing list" and related disclosures that we may make are limited by the Cable Act to disclosures of subscriber names and addresses where the disclosures do not reveal, directly or indirectly, (i) the extent of any viewing or other use by the subscriber of a cable service or other service provided by us; or (ii) the nature of any transaction made by the subscriber over our cable system.

We may sometimes disclose personally identifiable information about you to our affiliates or to others who work for us. We may also disclose personally identifiable information about you to outside auditors, professional advisors, service providers and vendors, potential business merger, acquisition, or sale partners, and regulators. We make these disclosures as provided for in the Cable Act. Typically, we make these disclosures when the disclosure is necessary to render, or conduct a legitimate business activity related to, the cable service or other services we provide to you. We may be required by law or legal process to disclose certain personally identifiable information about you to lawyers and parties in connection with litigation and to law enforcement personnel.

If we (or our parent company) enter into a merger, acquisition, or sale of all or a portion of our assets, subscribers' personally identifiable information will, in most instances, be one of the items transferred as part of the transaction. If this notice will be changed as a result of a transaction like that, you should refer below under "Will Comcast notify me if it changes this notice?"

We may also use or disclose personally identifiable information about you without your consent to protect our customers, employees, or property, in emergency situations, to enforce our rights under our terms of service and policies, in court or elsewhere, and as otherwise permitted by law.

When may Comcast disclose personal information to others in connection with phone service?

Comcast may disclose to others personally identifiable information in connection with features and services such as Caller ID, 911/E911, and directory services as follows:

- We may transmit your name and/or telephone number to be displayed on a Caller ID device unless you have elected to block such information. Please note that Caller ID blocking may not prevent the display of your name and/or telephone number when you dial certain business or emergency numbers, 911, 900 numbers, or toll-free 800, 888, 877, or 866 numbers.
- We may provide your name, address, and telephone number to public safety authorities and their vendors for inclusion in E911 databases and records, inclusion in "reverse 911" systems, or to troubleshoot 911/E911 record errors.
- We may publish and distribute, or cause to be published and distributed, telephone directories in print, on the Internet, and on disks. Those telephone directories may include subscriber names, addresses, and telephone numbers, without restriction to their use.
- We may also make subscriber names, addresses, and telephone numbers available, or cause such subscriber information to be made available, through directory assistance operators.
- We may provide subscribers' names, addresses, and telephone numbers to unaffiliated directory publishers and directory assistance providers for their use in creating directories and offering directory assistance services.
- Once our subscribers' names, addresses, and telephone numbers appear in telephone directories or directory assistance, they may be sorted, packaged, repackaged and made available again in different formats by anyone.

We take reasonable precautions to ensure that non-published and unlisted numbers are not included in our telephone directories or directory assistance services, but we cannot guarantee that errors will never occur.

When is Comcast required by law to disclose personally identifiable information and CPNI?

We make every reasonable effort to protect subscriber privacy as described in this notice. Nevertheless, we may be required by law to disclose personally identifiable information or individually identifiable CPNI about a subscriber. These disclosures may be made

with or without the subscriber's consent, and with or without notice, in compliance with the terms of valid legal process such as a subpoena, court order, or search warrant.

For subscribers to our cable television service, the Cable Act requires Comcast as a cable operator to disclose personally identifiable information to a third-party or governmental entity in response to a court order. If the court order is sought by a non-governmental entity, we are required to notify the subscriber of the court order. If the court order is sought by a governmental entity, the Cable Act requires that the cable subscriber be afforded the opportunity to appear and contest in a court proceeding relevant to the court order any claims made in support of the court order. At the proceeding, the Cable Act requires the governmental entity to offer clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case.

For subscribers to our high-speed Internet and phone services, the Cable Act requires Comcast to disclose personally identifiable information and individually identifiable CPNI to a private third party in response to a court order, and we are required to notify the subscriber of the court order. The Cable Act requires us to disclose personally identifiable information and individually identifiable CPNI about subscribers to high-speed Internet and phone services to a government entity in response to a subpoena, court order, or search warrant, for example. We are usually prohibited from notifying the subscriber of any disclosure of personally identifiable information to a government entity by the terms of the subpoena, court order, or search warrant.

How does Comcast protect personally identifiable information?

We follow industry-standard practices to take such actions as are necessary to prevent unauthorized access to personally identifiable information by a person other than the subscriber or us. However, we cannot guarantee that these practices will prevent every unauthorized attempt to access, use, or disclose personally identifiable information.

How long does Comcast maintain personally identifiable information?

Comcast maintains personally identifiable information about you in our regular business records while you are a subscriber to our cable service or other services. We also maintain this information for a period of time after you are no longer a subscriber if the information is necessary for the purposes for which it was collected or to satisfy legal requirements. These purposes typically include business, legal, or tax purposes. If these purposes no longer apply, we will destroy the information according to our internal policies and procedures.

IV. Customer Access and Choice

How can I see my personally identifiable information or CPNI and correct it, if necessary?

You may examine and correct, if necessary, the personally identifiable information regarding you that is collected and maintained by Comcast in our regular business records. In most cases, the personally identifiable information contained in these records consists solely of billing and account information. We will correct our records if you make a reasonable showing that any of the personally identifiable information we have collected about you is inaccurate.

If you have Internet access, you can view and change certain information yourself as follows:

- For accounts you have established at the Comcast.com website, use the Sign In or My Account (or similar) feature at www.comcast.com;
- For high-speed Internet accounts, use the Sign In or My Account (or similar) feature at www.comcast.net;
- For Comcast Digital Voice accounts, use the SmartZone Communications Center as applicable, using the Sign In or My Account (or similar) feature at www.comcast.net/digitalvoicecenter.

You may also examine the records containing your personally identifiable information at your local Comcast office upon reasonable prior notice to us and during our regular business hours. If you wish to examine these records, please contact us by mail or telephone at 1-800-COMCAST, giving us a reasonable period of time to locate and, if necessary, prepare the information for review, and to

arrange an appointment. You will only be permitted to examine records that contain personally identifiable information about your account and no other account.

If you make an affirmative, written request for a copy of your CPNI, we will disclose the relevant information we have to you at your account address of record, or to any person authorized by you, if we reasonably believe the request is valid. However, subscribers to our phone services should be aware that we generally do not provide them with records of any inbound or outbound calls or other records that we don't furnish in the ordinary course of business (for example, as part of a bill) or which are available only from our archives, without valid legal process such as a court order. In addition, we cannot correct any errors in customer names, addresses, or telephone numbers appearing in, or omitted from, our or our vendors' directory lists until the next available publication of those directory lists. Further, we may have no control over information appearing in the directory lists or directory assistance services of directory publishers or directory assistance providers which are not owned by us or our subsidiaries.

Comcast reserves the right to charge you for the cost of retrieving and photocopying any documents that you request.

How do I give or withhold my approval for Comcast to use CPNI to market additional products and services to me?

In addition to Comcast Digital Phone and Comcast Digital Voice, various direct and indirect subsidiaries of Comcast Corporation offer many communications-related services, such as Comcast High-Speed Internet services. From time to time we would like to use the CPNI information we have on file to provide you with information about our communications-related products and services or special promotions. Our use of CPNI may also enhance our ability to offer products and services tailored to your specific needs.

We would like your approval so that we, our agents, affiliates, joint venture partners, and independent contractors may use this CPNI to let you know about communications-related services other than those to which you currently subscribe that we believe may be of interest to you. IF YOU APPROVE, YOU MUST AFFIRMATIVELY TELL US BY OPTING IN TO THIS USE OF CPNI. You may approve (and later deny or withdraw a prior approval) our right to use your CPNI for this purpose by calling the numbers listed below. Our CPNI Policy contained in this notice is effective December 8, 2007.

Service	Call this Number
Comcast Digital Phone & Comcast Digital Voice	1-800-COMCAST
Comcast Business Communications & Comcast Long Distance	1-888-262-7300

Comcast also offers various other services that are not related to the services to which you subscribe. Under CPNI rules, some of those services, such as Comcast cable television services, are considered to be non-communications related products and services. Occasionally, you may be asked during a telephone call with one of our representatives for your oral consent to Comcast's use of your CPNI for the purpose of providing you with an offer for non-communications related products and services. If you provide your oral consent for Comcast to do so, Comcast may use your CPNI only for the duration of that telephone call in order to offer you additional services.

If you deny or restrict your approval for us to use your CPNI, you will suffer no effect, now or in the future, on how we provide any services to which you subscribe. Any denial or restriction of your approval remains valid until your services are discontinued or you affirmatively revoke or limit such approval or denial.

How do I place myself on Comcast's "do not call" and "do not mail" lists?

You may contact Comcast at 1-800-COMCAST to ask us to put your name on our internal company "do not call" and "do not mail" lists so that you do not receive marketing or promotional telephone calls or postal mail from us or made at our request. You also have the right to prohibit or limit disclosure of your personally identifiable information for "mailing list" or other purposes as described above in this notice by contacting us at 1-800-COMCAST.

Comcast's use of your account information for marketing and promotional activities is also subject to your right to limit or restrict us from making those offers as described above in "How do I give or withhold my approval for Comcast to use CPNI to market additional products and services to me?" in this notice.

If you prefer to contact Comcast in writing instead of by telephone, you may send a written request to the address listed below under "How do I contact Comcast?". Be sure to include your name and address, your Comcast account number, and a daytime telephone number where you can be reached in the event we have any questions about your request. The written request should be signed by the person who is identified in our billing records as the subscriber. If you have a joint account, a request by one party will apply to the entire account. If you have multiple accounts, your notice must separately identify each account covered by the request.

What e-mail communications will Comcast send to me and how do I manage them?

We may send a welcome e-mail and sometimes other information to new subscribers to our cable service and other services (including each new secondary account holder, where applicable). We may also send service-related announcements to our subscribers from time to time. For example, we may send you an e-mail announcement about a pricing change, a change in operating policies, a service appointment, or new features of one or more of the cable service or other services you receive from us. You may not opt-out of these service-related communications. If you fail to check your primary e-mail address for service-related announcements, you may miss important information about our services, including legal notices, for example.

We reserve the right to send you promotional or commercial e-mail as permitted by applicable law. You can manage the promotional or commercial e-mails Comcast may send to you by following the instructions contained in the e-mails or by going to the web page located at www.comcast.com/preferences and following the directions there. We may ask for additional information on this preferences page such as your zip code, for example. By providing this additional information to us we will be able to better inform you of the availability of special offers and promotions in your area. If you no longer wish to receive these e-mails you may opt-out of receiving them by going to the same page and changing your contact preferences.

What can I do if I think my privacy rights have been violated?

If you believe that you have been aggrieved by any act of ours in violation of the Cable Act, we encourage you to contact us directly as described below in "How do I contact Comcast?" in order to resolve your question or concern. You may also enforce the limitations imposed on us by the Cable Act as applicable with respect to your personally identifiable information through a civil lawsuit seeking damages, attorney's fees, and litigation costs. Other rights and remedies may be available to you under federal or other applicable laws as well.

Will Comcast notify me if it changes this notice?

As required by the Cable Act, we will provide you with a copy of this customer privacy notice at the time we enter into an agreement to provide any cable service or other service to you, and annually afterwards, or as otherwise permitted by law. You can view the most current version of this notice by going to www.comcast.com, searching for "privacy policy," and selecting the appropriate link.

We may modify this notice at any time. We will notify you of any material changes through written, electronic, or other means and as otherwise permitted by law. If you find the changes to this notice unacceptable, you have the right to cancel your service. If you continue to use the service following notice of the changes, we will consider that to be your acceptance of and consent to the changes in the revised privacy notice. This includes your consent for any personally identifiable information that we may collect and use starting on the effective date of the revised notice, as well as for any personally identifiable information that we have collected prior to the effective date of the revised notice. However, we will only consider your continued use of the service to be your acceptance of and consent to changes in the revised privacy notice for changes made after December 31, 2006.

How do I contact Comcast?

If you have any questions or suggestions regarding this privacy notice, or wish to contact us about your personal information, please reach us as follows:

Phone: 1-800-COMCAST

Web site: www.askcomcast.com/contactus.asp

Mail: Comcast Cable Communications, LLC

References

Blanke, Jordan M. "Minnesota passes the nation's first Internet privacy law". Rutgers Computer & Technology Law Journal, <http://www.entrepreneur.com/tradejournals/article/106474530.html> (accessed September 26, 2010).

Bradley, Tony. About.com. "What is Two-Factor Authentication?" *Understanding what two-factor authentication is and how it works*. <http://netsecurity.about.com/od/quicktips/qt/twofactor.htm> (accessed November 14, 2010).

CALEA – Definition. wordIQ.com. <http://wordiq.com/definition/CALEA> (accessed November 3, 2010).

California Department of Motor Vehicles. "Government Requester Accounts." <http://www.dmv.ca.gov/otherser/gra/govreq.htm> (accessed December 19, 2010).

Cox Communication, Inc. "Cox Communication LEA Information Policy", last modified October 1, 2009. *Notice to parties serving subpoenas on Cox Communication*. <http://cryptome.org/isp-spy/cox-spy.pdf>. (accessed October 1, 2010).

Curtis, Kathleen. Phone interview. Kathleen Curtis, Bureau of Motor Vehicles, State of Maine. (Oct. 7, 2010).

Dahlia Lithwick and Julia Turner. "A Guide to the Patriot Act, Part 1, Should you be Scared of the Patriot Act?" <http://www.slate.com/id/2087984/> (accessed October 1, 2010).

DCS.com. "Scope and impact of the European Data Retention Directive." 16 January 2007. http://datacentresols.com/news_full.php?id=9515&title=Scope-and-impact-of-the-European-Data-Retention-Directive. (accessed September 29, 2010).

Department of Driver Services. "How do I request a driver history report (MVR)?" December 13, 2010. <http://www.dds.ga.gov/drivers/DLdata.aspx?con=1740840381&ty=dl> (accessed December 28, 2010).

Epic.org. *The Drivers Privacy Protection Act (DDPA) and the Privacy of Your State Motor Vehicle Record*. Electronic Privacy Information Center. <http://epic.org/privacy/drivers/> (accessed October 11, 2010).

Epic.org. "Cable TV Privacy Act of 1984." *Electronic Privacy Information Center*, http://epic.org/privacy/cable_tv/ctpa.html. (accessed October 11, 2010).

FCC 06-56. Federal Communication Commission. "Second Report and Order and Memorandum Opinion and Order", May 3, 2006. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-56A1.pdf (accessed November 7, 2010).

Federal Communications Commission. "Telecommunications Act of 1996." <http://www.fcc.gov/telecom.html> (accessed October 4, 2010).

Federal Communications Commission. "Understanding your Telephone Bill." *FCC Consumer Facts*. <http://www.fcc.gov/cgb/consumerfacts/understanding.html> (accessed October 30, 2010).

Free Dictionary Online. Legal definition of Contraband. <http://legal-dictionary.thefreedictionary.com/contraband>. (accessed November 2, 2010).

IBM®. "IBM Security." <http://www-03.ibm.com/systems/z/advantages/security/index.html> (accessed November 12, 2010).

Information Sciences Institute, University of Southern California. *Internet Protocol. Darpa Internet Program Protocol Specification*. <http://www.ietf.org/rfc/rfc791.txt> (accessed January 2011).

Internet World Stats Usage and Population Statistics. "United States of America Internet Usage and Broadband Usage Report" <http://www.internetworldstats.com/am/us.htm> (accessed October 11, 2010).

IRS.gov. "IRS e-file: Secure Online Tax Filing". <http://www.irs.gov/efile/article/0,,id=121477,00.html> (accessed October 2, 2010).

King, Stan H. January 11, 2010. "Mainframe Hacking: Fact or Fiction?" <http://www.mainframezone.com/it-management/mainframe-hacking-fact-or-fiction> (accessed November 12, 2010).

KOLD, News 13®. "IRS E-File, Free File and other electronic options", IRS.gov. <http://www.kold.com/Global/story.asp?S=1072219> (accessed October 1, 2010).

Korzeniewski, Jeremy. Nov 5, 2010. "Polk: People continuing to keep vehicles longer." <http://www.autoblog.com/2010/11/05/polk-people-continuing-to-keep-vehicles-longer/>. (accessed December 13, 2010).

Lang, Glen. Phone interview. Sergeant Glen Lang, Maine State Computer Crimes Unit. (6 Oct. 2010).

Lie, David and John Maly. Stanford University. May 27, 2000. EE482: "Advanced Computer Organization Processor Architecture." *Reliability, Availability, and Serviceability*. <http://cva.stanford.edu/classes/ee482a/scribed/lect16.pdf> (accessed November 12, 2010).

Meierhoefer, Cameron. October 12, 2010. comScore Voices. "comScore September 2010 qSearch Reporting Enhancements." <http://blog.comscore.com/meirhoefer.html>. (accessed December 13, 2010).

Microsoft Corporation©. 2011. "Maximum Capacity Specifications for SQL Server." [http://msdn.microsoft.com/en-us/library/ms143432\(printer\).aspx](http://msdn.microsoft.com/en-us/library/ms143432(printer).aspx) (accessed November 12, 2010).

Neurstar.com. "When law enforcement calls, will you be ready?" <http://www.neustar.biz/services/legal-compliance-services/court-ordered-records-production> (accessed December 28, 2010).

O'Connell, Kelly. "Internet Law – NJ Supreme Court Says Subpoena Needed for Internet Records." *Internet Business Law Services*. http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2043 (accessed September 26, 2010).

Parr, Ben. "UK Passes Controversial Digital Economy Bill." <http://mashable.com/2010/04/07/digital-economy-bill/>. (accessed October 3, 2010).

Photo Attorney® "The Cost of Copyright Infringement." <http://www.photoattorney.com/2007/10/costs-of-copyright-infringement.html> (accessed October 3, 2010).

Racoma, J. Angelo. November 3, 2010. "Chevy Volt Electric Cars Each Have Their Own IP Addrss." *IBM & GM Say Volt's Electronic Control Unit has 10M Lines of Code & Own IP Address*. <http://nexus404.com/Blog/2010/11/03/chevy-volt-electric-cars-each-have-their-own-ip-address-ibm-gm-say-volts-electronic-control-unit-has-10m-lines-of-code-own-ip-address/> (accessed December 27, 2010).

Radding, Alan. July 22, 2010. Big Fat Finance Blog. "Mainframe 101 for C-Level Executives." <http://bigfatfinanceblog.com/2010/07/22/mainframe-101-for-c-level-executives/> (accessed November 12, 2010).

RidgeviewTel™ LLC. "Privacy Policy". <http://www.myridgeviewtel.com/site-policy.php> (accessed December 27, 2010).

State of California Department of Motor Vehicle. "Information Security Statement." <http://www.dmv.ca.gov/forms/inf/inf1128.pdf> (accessed December 28, 2010).

States and Education – State Administrative Services in Education.

<http://education.stateuniversity.com/pages/2449/States-Education-STATE-ADMINISTRATIVE-SERVICES-IN-EDUCATION.html> (accessed December 28, 2010).

Timeanddate.com. "GMT – Greenwich Mean Time."

<http://www.timeanddate.com/library/abbreviations/timezones/eu/gmt.html> (accessed November 3, 2010).

Time Warner Cable. Subscriber Statement. January 1, 2011

University of Kansas. Center for Teaching Excellence. "Special Districts."

www.cte.ku.edu/.../Presentation%20Example%204%20Special%20Districts.ppt (accessed December 28, 2010).

US Department of Justice. 18 U.S.C. 2703. Requirements for Governmental Access.

<http://justice.gov/criminal/cybercrime/usc2703.htm> (accessed September 30, 2010).

US Department of Justice. "Electronic Communications Privacy Act of 1986." *Justice*

Information Sharing. <http://it.ojp.gov/default.aspx?area=privacy&page=1285>. (accessed October 3, 2010).

Wikipedia.com. "Evaluation Assurance Level".

http://en.wikipedia.org/wiki/Evaluation_Assurance_Level (accessed November 12, 2010).

Wikipedia.com. "IPv4 address exhaustion."

http://en.wikipedia.org/wiki/IPv4_address_exhaustion (accessed December 27, 2010).

Wikramanayake, G. N. and J.S. Goonetillake. "Managing Very Large Databases and Data Warehousing." University of Colombo School of Computing.

<http://www.cmb.ac.lk/academic/institutes/nilis/reports/gihan.pdf> (accessed December 22, 2010).

World Internet Usage Statistics News and World Population Stats. "Internet Usage Statistics,

The Internet Big Picture." <http://www.internetworldstats.com/stats.htm> (accessed October 11, 2010).

Yahoo Answers.com. "How many different ZIP codes are there in New York City?"

<http://answers.yahoo.com/question/index?qid=20070320141640AAcuLmf> (accessed November 3, 2010).

Zonk. "US Government Demands Data Retention." (June 2, 2008), Slashdot.com. (accessed October 19, 2010).