

**TESTIMONY OF
MICHAEL J. WOODS
VICE PRESIDENT & ASSOCIATE GENERAL COUNSEL
VERIZON COMMUNICATIONS INC.**

BEFORE THE

**SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE**

“FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) REFORMS”

JUNE 5, 2014

I am pleased to testify before the Committee on the topic of Foreign Intelligence Surveillance Act reforms. My name is Michael Woods. I am a Vice President and Associate General Counsel of Verizon. I lead Verizon’s national security and public safety policy teams and provide legal advice to Verizon components engaged in these areas. Prior to serving in this role at Verizon, I served as counsel in the Office of Law & Policy of the National Security Division at the Justice Department; as chief of the National Security Law Unit at the FBI; as counsel to the National Counterintelligence Executive; and as a Department of Justice environmental crimes prosecutor.

Two weeks ago, the House of Representatives passed legislation (H.R. 3361, the USA FREEDOM Act) aimed at creating stronger privacy protections for American citizens by ending the collection of bulk data by U.S. intelligence agencies and bringing greater transparency to the surveillance process, among other things.

Verizon supports this legislation for several reasons. Customer privacy is a top priority for Verizon and we believe that this legislation properly strengthens privacy protections. It also improves procedural transparency and does not require telecommunications companies to retain data beyond what they do today for business purposes. While recognizing that Congress is best positioned to balance competing national security and privacy concerns, our sense is that the legislation's privacy protections can be achieved without compromising the security of the American people.

The Primacy of Privacy Protection

Congress has long recognized that telecommunications carriers have access to information that can help national security and law enforcement officials save lives and/or avert threats to public health, safety and economic well-being. Verizon has devoted substantial resources to ensure its lawful compliance with national security and law enforcement requests.

That said, Verizon is committed to maintaining strong and meaningful privacy protections for our customers. Our privacy policy is designed to inform them about the information we collect, how we use it, and their options about certain uses of information. This information is used to deliver, provide, and repair products or services; establish and maintain customer accounts and billing records; contact them about our products and services and offers or promotions; and manage and protect our networks. A copy of Verizon's privacy policy is attached.

We are also committed to protecting the security of our customer information. Verizon has technical, administrative and physical safeguards in place to help protect against unauthorized access to, use or disclosure of customer information we maintain.

Ensuring that every national security or law enforcement request for information is in full compliance with the law is an obligation Verizon takes very seriously on behalf of our customers. While we have a legal obligation to provide customer information to law enforcement in response to lawful demands, we take seriously our duty to provide such information *only* when authorized by law. Our dedicated teams carefully review each demand and reject those that fail to comply with the law. If a demand is overly broad or vague, we will not disclose any information in response or will work to narrow the scope of the information we produce. Some demands seek information that we simply do not have; accordingly, we produce no information at all or only some of the information sought by those demands from law enforcement.

Verizon views the FISA business record reforms in H.R. 3361 as consistent with appropriate privacy protections.

The Importance of Improved Transparency

Provisions of H.R. 3361 (as well as similar Senate legislation) allow for additional reporting on orders requiring the production of business records. Such transparency promotes the accountability of U.S. surveillance efforts and should help promote public trust. Verizon has been an industry leader in this area and published our first

transparency report in January 2014. This report was praised at the time by groups like the Center for Democracy and Technology as setting a precedent for transparency in the industry. A copy of that report is attached.

At the time we issued our transparency report, we were not permitted to report information on national security requests other than a broad range for the number of National Security Letters we received from the FBI. In February 2014 the Department of Justice issued guidance allowing companies to report some information on national security matters, and we updated our transparency report with this information in early March (also attached). We will update our transparency report again this Summer.

While Verizon and several other companies have decided to provide data on requests from law enforcement, these efforts still provide an incomplete picture of government action, given the vast number of telecommunications and Internet companies around the world that are not publically reporting this information. The only truly comprehensive and uniform data set is in the hands of the governments themselves, and we call on all governments to make public the number of demands they make for customer data from telecommunications and Internet companies.

The U.S. government is well-positioned to produce such a report. A framework already exists for it to report to Congress on the number of wiretap orders, pen register and trap and trace orders, certain emergency requests and national security letters. The U.S. government should expand on this existing framework and report annually on the

numbers of all types of demands made by federal and state law enforcement to telecommunications and Internet companies for data regarding their customers.

The Inappropriateness of Outsourcing Surveillance

Included in the reform discussions has been the idea that the collection, searching, and perhaps even analysis, of potentially relevant data is best done not by the government, but by the private holders of that data. One recommendation that garnered particular attention was that bulk collection of telephony metadata might be replaced by a system in which such metadata is held instead either by private providers or by a private third party.

This proposal opens a very complex debate, even when that debate is restricted to just traditional telephony, but the bottom line is this: national security is a fundamental government function that should not be outsourced to private companies.

Verizon is in the business of providing communications and other services to our customers. Data generated by that process is held only if, and only for as long as, there is a business purpose in doing so. Outside of internal business operations, there typically is no need for companies to retain data for extended periods of time.

If a company is required to retain data for the use of intelligence agencies, it is no longer acting pursuant to a business purpose. Rather, it is serving the government's purpose. In this context, the company has become an agent or surrogate of the government. Any Constitutional benefit of having the data held by private entities is

lost when, by compelling retention of that data for non-business purposes, the private entity becomes a functional surrogate of the government. Public trust would exist to the extent that companies are believed to be truly independent of the government. When the companies are seen as surrogates for intelligence agencies, such trust will dissipate.

Nor would outsourcing offer any promise of efficiency. Technology is changing too rapidly -- telecommunications networks are evolving beyond traditional switched telephony. Voice over Internet Protocol (VoIP) technologies handle voice traffic over the Internet (as opposed to the public switched telephone networks) and already account for a substantial portion of voice traffic. Even more dramatic has been the rise of "over-the-top" applications that use peer to peer or other technologies to establish direct connections between users over the Internet. In 2012, one such application accounted for 34% of all international voice calling minutes. VoIP and over-the-top applications traverse IP networks as Internet traffic and thus do not generate CDRs or similar telephony business records. U.S. intelligence agencies would need to approach application owners to establish access equivalent to the CDRs they obtain under the existing program. The technical difficulties multiply if the intelligence agencies were to eventually seek the same sort of access to IP metadata from Internet Service Providers.

Finally, the commercial effect on U.S. companies of outsourcing collection ought to be considered. No company will be eager to undertake the increased responsibility, scrutiny, and liability entailed by having its employees become surrogates for the

government in the collection of intelligence. More troubling for large companies is the negative effect in the international market of overt association with a U.S. intelligence agency.

H.R. 3361 does not include any provisions which would require data retention by telecommunications companies. For all of the foregoing reasons, that is a good thing. A framework under which intelligence agencies retain and analyze data that has been obtained from telecommunications companies in a "arms length" transaction compelled by a FISA order should continue.

Conclusion

Verizon supports Congressional efforts to rebalance national security and privacy interests in the aftermath of the NSA surveillance disclosures. Critical policy objectives include improving privacy protections and procedural transparency, ensuring appropriate liability protections, and maintaining a structure that does not require private sector organizations to act as surrogates for U.S. intelligence agencies.



Privacy Policy

Full Privacy Policy

- [Privacy Policy Summary](#)
- [Full Privacy Policy](#)
- [Privacy Officer Message](#)
- [Recent Changes to the Policy](#)
- [Tips for Guarding Your Information](#)
- [FiOS Privacy Policy](#)
- [Browser Policy Statement](#)
- [Your California Privacy Rights](#)
- [Your Ohio Rights & Responsibilities](#)



Verizon Participates in the TRUSTe Privacy Program

[\[more \]](#)



Verizon is accredited by the Better Business Bureau Online (BBBOnline)

[\[more \]](#)

Verizon is Committed to Protecting Your Privacy

Protecting our customers' privacy is an important priority at Verizon and we are committed to maintaining strong and meaningful privacy protections. The privacy of your information is a significant responsibility and we value the trust you place in us.

Our Privacy Policy is designed to inform you about the information we collect, how we use it, and your options with regard to that collection and use. This policy also describes privacy rights you have under certain federal laws.

This policy applies to Verizon customers in the United States and to visitors to Verizon websites. For Verizon Business customers outside the United States, policies are set forth at <http://www.verizonenterprise.com/terms/>. Also, certain services offered to consumers as well as contracts between Verizon and its business customers (both U.S. and international) may contain additional privacy-related terms and conditions. Except as described above, this policy applies across the [Verizon family of companies](#) and the products and services they provide. The Verizon family of companies includes the companies and joint ventures controlled by Verizon, including the Verizon telephone companies, Verizon Wireless, Verizon Online and Redbox Instant by Verizon.

This policy also includes additional privacy practices that are applicable to specific Verizon offerings such as FiOS, Wireless and Redbox Instant by Verizon services.

[Back to Summary](#)

Information We Collect and How We Use It

We collect and use information about you in the following ways:

Information Collected When You Communicate with Verizon:

When you communicate with Verizon, we collect information from you that we use to deliver, provide, confirm, change, bill, monitor, maintain and repair your products and services. This information is also used to resolve issues with your order, with our products and services, or with your account. The information we collect may include your name, addresses, and other contact information; the reason for the contact; and your driver's license number and Social Security Number and payment information. We use this information to establish and maintain your customer account and billing records (including establishing credit), provide services to you, authenticate you, and contact you about products and services that we offer.

When you contact us or we contact you with calls, e-mail, in writing, or through a feature on our websites or in our applications, we may monitor or record that communication or keep a record of the transaction to help us train employees and provide high-quality customer service.

Information Collected When You Use Verizon Products and Services:

We collect information about your use of our products, services and sites. Information such as call records, websites visited, wireless location, application and feature usage, network traffic data, product and device-specific information, service options you choose, mobile and device numbers, video streaming and video packages and usage, movie rental and purchase data, FiOS TV viewership, and other similar information may be used for billing purposes, to deliver and maintain products and services, or to help you with service-related issues or questions. In addition, this information may be used for purposes such as providing you with information about product or service enhancements, determining your eligibility for new products and services, and marketing to you based on your use of your products and services. This information may also be used to manage and protect our networks, services and users from fraudulent, abusive, or unlawful uses; and help us improve our services, research and develop new products, and offer promotions and other services.

If you subscribe to Verizon Internet access services, we may automatically measure and monitor network performance and the performance of your Internet connection to improve your, or our, service levels and products. If you contact us for service support, we also may access information about your computer, wireless device or other device settings to provide customized technical support or to install specific applications or services that you use or that are necessary to the applications or services you use.

This type of information may be aggregated or anonymized for business and marketing uses by us or by third parties. For example, aggregate or anonymous data may be used to improve our services, measure and analyze the use of services and to help make services and advertising more relevant to customers.

When you establish an online account with us, we maintain information about your user identification and password. This information is used to identify you when you sign in to your account.

If Verizon intends to gather information from your use of our Internet access services to direct customized advertising specifically to you based on your visits over time and across different non-Verizon websites, we will provide you with notice of our plan and obtain your affirmative consent.

Please note that Verizon is not responsible for information, content, applications or services provided by others. Before you access, use, link to or download a service or application on your computer, television, wireless or other device, you should review the associated terms of service and privacy policy. Personal information you submit in these contexts may be read, collected or used by the service or application provider and others associated with these forums in a manner different from that described here.

Information Provided to Us by Third Parties:

When you purchase products or apply for service with us, we may obtain credit information about you from outside credit reporting agencies to help us with customer authentication and credit-related decisions. If you lease your residence, we may have information about how to reach your landlord and whether landlord permission is required to install our

facilities.

Verizon obtains information from outside companies that collect consumer information such as demographic and interest data. Examples of this information include gender, age range, sports enthusiast, frequent diner or pet owner. We use this data and combine it with other information we have about you to help us predict customer preferences and to direct marketing offers that might be more relevant to you.

When you use social media credentials to login to or otherwise interact with a Verizon site or offer, we may collect information about your social media profile, such as your interests, "likes" and friends list. We may use this information, for example, to personalize your Verizon experiences and marketing communications, to enhance our services and to better serve you. You can control this data sharing via options in your social media accounts.


We may also obtain contact information and other marketing lead information from third parties, and may combine it with information we have to contact you or direct Verizon's marketing offers to you. Website visitors and others may provide us with your email address through "refer-a-friend" options or social networking platforms. We use these email addresses to send Verizon promotional marketing information.

Information Collected on Verizon Websites:

When you browse Verizon websites, information is collected about your device and your visit. We also collect data about your browsing, searching and buying activity as you interact with our sites. We may collect and use your IP address, mobile telephone or device number, account information, web addresses of the sites you come from and go to next and information about your connection, including your device's browser, operating system, platform type and Internet connection speed. We use this information for operational and performance measurement purposes including monitoring statistics such as how many people visit our websites; which pages people visit on our site; how much time is spent on each page or; which browsers are used to visit our sites.

Verizon and its vendors also use information collected on Verizon websites to help us deliver more relevant Verizon marketing messages. These messages may be delivered on our websites, on non-Verizon websites, by our representatives, via email, or via other Verizon services or devices. We use this information in order to, among other things, ensure that you see the correct products and pricing available in the geographic area in which you live, manage the frequency with which you see an advertisement, tailor advertisements to better match your interests, and to understand the effectiveness of our advertising. We also may use this information to assess the effectiveness of our sites and to help you should you request help with navigation problems on these sites.

Certain Verizon vendors may place and read **cookies** on our sites to help us deliver Verizon marketing messages on our sites and on non-Verizon sites. We require that these vendors provide consumers with the ability to opt-out of their use of information for these purposes. In accordance with **industry self-regulatory principles**, you should see this icon

 In or around Verizon advertisements that are delivered on other sites using information collected on our sites. Clicking on this icon will provide information about the companies and data practices that were used to deliver the ad and will also describe how you may opt-out of these advertising programs. Additional information on the choices available to you for the use of your information for advertising purposes can be found in the "How to Limit the Sharing and Use of Your Information" section below.

[Additional information about "cookies" and related technologies](#)

When you register on our sites, we may assign an anonymous, unique identifier. This may allow select advertising entities to use information they have about your web browsing on a desktop computer to deliver marketing messages to mobile devices on our network. We do not share any information that identifies you personally outside of Verizon as part of this program. You have a choice about whether to participate, and you can visit our relevant mobile advertising page (link to www.vzw.com/myprivacy) to learn more or advise us of your choice.

[Back to Summary](#)

Information You Provide:

When you contact us online or by other means for information about products and services or when you enter a Verizon-sponsored or affiliated contest, sweepstakes or similar promotion, we will respond to your request and may use the information you supply us to provide you with additional information about service offerings either at that time or in the future. If you enter a promotion, your information may be disclosed as part of the program's administration, such as in connection with the publication of winners, prize fulfillment, and as required by law or permitted by the promotion's official rules. Information you provide on our websites about your preferred location and other preferences may be used to provide you with more relevant product recommendations, services and special offers.

If you provide information to us in the context of an event that Verizon sponsors with another organization, such as a contest or sweepstakes, or if you visit a co-sponsored site or use a co-sponsored service, you also may be providing information to the co-sponsor. You should refer to that co-sponsor's privacy policy for information about its practices which may differ from Verizon's practices.

We may also collect information from you when you agree to participate in surveys or provide other feedback to us regarding our products or services, when you register to receive news or public policy updates, or when you apply for a job with or a grant from Verizon. We use this information only for the purpose for which you provide it.

Verizon may send you emails that communicate information about your account or about products, services, marketing offers, or promotions that may be of interest to you. When you open a Verizon email or click on links within these emails, we may collect and retain information to provide you with future communications that may be more interesting to you. Please note that Verizon will not ask you to send us, via email, sensitive personal or account information.

[Back to Summary](#)

Additional Information for Wireless Customers

Verizon Wireless collects and uses mobile device location data for a variety of purposes, including to provide our mobile voice and data services, emergency services, and our and third-party location-based applications and services such as navigation, weather, mapping and child safety applications or tools. Where we offer our own location-based applications, we provide you with notice and choice about whether specific location-tracking features available on your device are turned on.

Many types of wireless applications and services use mobile device location data, including applications provided by other companies and wireless device operating systems. When you are considering new applications or services, you should carefully review the location-based services' or application providers' privacy policies to learn how they collect and use your information.

Verizon Wireless may use mobile usage information and consumer information for certain business and marketing reports. Mobile usage information includes the addresses of websites you visit when you use our wireless services. These data strings (or URLs) may include search terms you have used. Mobile usage information also includes the location of your device and your use of applications and features. Consumer information includes information about your use of Verizon products and services (such as data and calling features, device type, and amount of use) as well as demographic and interest categories provided to us by other companies (such as gender, age range, sports fan, frequent diner, or pet owner). We may combine this information in a manner that does not personally identify you and use it to prepare aggregated business and marketing reports that we may use ourselves or share with others for their use. We may also share location information with other companies in a way that does not personally identify you so that they may produce business and marketing reports. You have a **choice** about whether your information is included in these reports.

Verizon Wireless does not publish directories of our customers' wireless phone numbers, and we do not provide or make them available to third parties for listing in directories unless you request that we do so.

[Back to Summary](#)

Information About the Cable Act

To the extent that Section 631 of the Communications Act of 1934, as amended (the "Cable Act") applies to services you purchase, it entitles you to know about the personally identifiable information a cable service provider collects. This includes the nature of the use and disclosure of this information and to whom it may be disclosed, how long personally identifiable information is maintained, and how subscribers may access it. In addition, the Cable Act imposes limits on the collection and disclosure of personal information and gives subscribers the ability to enforce their privacy rights. (Personally identifiable information does not include aggregate data that does not identify a particular person).

The Cable Act allows a provider to use its cable system to collect personally identifiable information necessary to render a cable service or other services provided to subscribers and to detect and prevent unauthorized access to services. Additional personally identifiable information may be collected with the subscriber's prior consent. Personally identifiable information may be used or disclosed without the subscriber's consent where necessary to render services, and to conduct legitimate business activities related to services provided. We may be required by law to disclose personally identifiable information to a governmental entity to comply with valid legal process, such as warrants, court orders or subpoenas, but we will not disclose records revealing your selection of video programming unless we receive a court order indicating that the governmental entity has made a specified showing of relevance and you were afforded an opportunity to contest the order. We may be required to disclose personally identifiable information (including your selection of video programming) to a non-governmental entity to comply with a court order, after you have been provided notice.

If you believe that your privacy rights have been violated, please contact us at privacyoffice@verizon.com and we will work with you to address your concerns. If you believe that you have been aggrieved as a result of a violation of the Cable Act, you may enforce the limitations imposed by the Cable Act through a civil action in a United States district court seeking damages, attorney's fees, and litigation costs. Other rights and remedies may also be available to you under federal or other applicable laws.

The Cable Act permits the disclosure of customer names and addresses as long as a subscriber has been provided with the opportunity to prohibit or limit this disclosure and the disclosure does not reveal, directly or indirectly, the subscriber's viewing or other uses of the cable or other services provided. If we intend to share data in this way, we will provide you with the opportunity to prohibit or limit this type of sharing.

Relevant TV Advertising

Verizon's Relevant TV Advertising program helps advertisers reach FIOS television customers with advertisements that may be more relevant to their interests. We do not share any information that identifies you personally outside of Verizon as part of this program. The ads may appear on a variety of platforms where FIOS television customers can access video content. We help advertisers deliver ads to audiences based on demographic and interest information (such as gender, family size, and luxury car owner) we obtain from other companies, your address and certain information about your Verizon products and services (such as service packages purchased, video on-demand purchases, and program viewing data). You have a choice about receiving this type of advertising and you can opt out [online](#).

Additional Information for Redbox Instant by Verizon Customers

Redbox Instant by Verizon video streaming services are offered through a joint venture between Verizon and Redbox. When you subscribe to or use Redbox Instant by Verizon

services, your information is shared with both Verizon and Redbox and is covered by this privacy policy as well as [Redbox's privacy policy](#). Redbox Instant by Verizon services will be available to you through websites and Internet-connected device platforms operated by other companies such as gaming devices, streaming video devices, tablets and wireless phones. When you access Redbox Instant by Verizon on others' websites or platforms, you should check these providers' privacy policies to learn what information they collect and use.

[Back to Summary](#)

Information We Share

Information Shared Within the Verizon Family of Companies:

Verizon shares customer information within our family of companies. You can limit our sharing of certain types of customer information, known as Customer Proprietary Network Information, for marketing purposes as described more fully below. Sharing this information allows us to provide you with the latest information about our products and services and to offer you our latest promotions.

Additional protections apply for certain information we collect and maintain about the telecommunications and Voice over Internet Protocol (VoIP) services you buy from us and how you use them. This information is categorized by the federal government as [Customer Proprietary Network Information](#) or CPNI. Specific laws govern our sharing and use of this type of information.

Verizon Wireless and Wireline residential customers as well as Verizon Wireline small and medium business customers receive a privacy notice regarding CPNI when they first contract for or order service and at least every two years thereafter. For more information, please read the [Verizon Wireline](#) and [Verizon Wireless](#) CPNI notices. You may [choose to opt out](#) of the sharing of your CPNI within the Verizon family of companies for certain marketing purposes.

Our corporate and government account customers in the United States receive a CPNI consent form or service agreement requesting affirmative approval to share CPNI information. As described in the request, you may decline or withdraw CPNI consent by not signing the consent form or by following instructions in the consent form or service agreement. Your choice on CPNI consent will remain in effect unless you change it.

If you are an Arizona resident, as required by state law, Verizon Wireless does not share your CPNI within the Verizon family of companies [unless you provide consent](#). Customers who provide such consent are reminded annually of their current CPNI choices.

If you are a retail customer of MCI, your CPNI will not be shared within the Verizon family of companies for marketing purposes except to provide you with information about other services of the type you currently buy from us. In addition, when you are speaking with a customer service representative, we may ask your permission to review your records, including your CPNI, to provide you with information about the full array of services provided by the Verizon family of companies.

Information Shared Outside the Verizon Family of Companies:

Except as explained in this Privacy Policy, in privacy policies for specific services, or in agreements with our customers, Verizon does not sell, license or share information that individually identifies our customers, people using our networks, or website visitors with others outside the Verizon family of companies for non-Verizon purposes without the consent of the person whose information will be shared.

Verizon uses vendors and partners for a variety of business purposes such as to help us offer, provide, repair and bill for services we provide. We share information with those vendors and partners when it is necessary for them to perform work on our behalf. For example, we may provide your credit card information and billing address to our payment processing company solely for the purpose of processing payment for a transaction you have requested. We require that these vendors and partners protect the customer information we provide to them and limit their use of Verizon customer data to the purposes for which it was provided. We do not permit these types of vendors and partners to use this information for their own marketing purposes.

As described in more detail in other sections of this policy, Verizon also may share certain information with outside companies—, for example, to assist with the delivery of [advertising campaigns](#), or preparing and sharing aggregate reports.

Verizon provides the names, addresses and telephone numbers of wireline telephone customers to directory publishers and directory assistance services unless a non-published or non-listed phone number has been requested.

We may disclose information that individually identifies our customers or identifies customer devices in certain circumstances, such as:

- to comply with valid legal process including subpoenas, court orders or search warrants, and as otherwise authorized by law;
- in cases involving danger of death or serious physical injury to any person or other emergencies;
- to protect our rights or property, or the safety of our customers or employees;
- to protect against fraudulent, malicious, abusive, unauthorized or unlawful use of or subscription to our products and services and to protect our network, services, devices and users from such use;
- to advance or defend against complaints or legal claims in court, administrative proceedings and elsewhere;
- to credit bureaus or collection agencies for reporting purposes or to obtain payment for Verizon-billed products and services;
- to a third-party that you have authorized to verify your account information;
- to outside auditors and regulators; or
- with your consent.


When you purchase services offered jointly by Verizon and one of our partners, customer information may be received by both Verizon and our partner that is providing your service. For these jointly offered services, you should also review the partner company's privacy policy which may include practices that are different from the practices described here. If Verizon enters into a merger, acquisition or sale of all or a portion of its assets or business, customer information will also be transferred as part of or in connection with the transaction.

Information Provided to or Used by Third-Party Advertising Entities or Social Networks

You may see third-party advertisements on some Verizon websites, services, or devices. Some advertisements are chosen by companies that place advertisements on behalf of other third-party advertisers. These companies, often called ad servers, ad networks, or technology platforms, may place and access cookies on your device to collect information about your visit on our websites. The information they collect from our sites is in a form that does not identify you personally. This information may be combined with similar data obtained from other websites to help advertisers better reach their targeted audiences. Targeting may be accomplished by tailoring advertising to interests that they infer from your browsing of our sites and your interaction with other websites where these ad servers, ad networks and technology platforms also are present.

If you choose to interact with specific advertisers who advertise on our sites or services, the information you provide to them is subject to the conditions of their specific privacy policies. In addition, responding to or interacting with a particular advertisement, may result in you later receiving a targeted advertisement on our websites or on other sites as a result of an ad server or ad network concluding that you fit within a particular audience an advertiser is trying to reach.

Advertising that is customized based on predictions generated from your visits over time and across different websites is sometimes called "online behavioral" or "interest-based" advertising. In accordance with [industry self-regulatory principles](#), we require that companies disclose when they are using online behavioral advertising programs to deliver third-party ads on our sites or collecting information about your visit to our sites for these purposes and give consumers the ability to opt-out of this use of their information. You will see

an icon  in or around third-party advertisements that are delivered on our sites using behavioral advertising programs. Clicking on this icon will provide additional information about the companies and data practices that were used to deliver the ad as well as information on how you may opt-out of these advertising programs. Additional information about your options regarding the use of your information for advertising purposes can be found [below](#). Additional information about online behavioral advertising can be found [here](#). Please note that Verizon does not have control over or access to information contained in the cookies that are set on your computer by ad servers, ad networks or third-party advertisers.

Additional information about "cookies" and related technologies

We also may provide third-party advertisers with geographic or demographic information that allows them to tailor their ads. This information does not identify you individually. Verizon also helps advertisers better reach our wireline and wireless Internet access customers using the postal address we have for you; certain information about your Verizon products and services—such as device type and broadband service features; and demographic and interest information provided to us by other companies—such as gender, age-range, sports fan, frequent diner or pet owner. This information is used to predict whether you fit within an audience an advertiser is trying to reach. In addition, using an anonymous, unique identifier we create when you register on our websites, we may allow an advertiser to use information they have about your visits to websites on a desktop computer to deliver marketing messages to mobile devices on our network. We do not share outside of Verizon any information that identifies you personally as part of these programs. You have a [choice](#) about participating in the separate [Verizon](#) and [Verizon Wireless](#) programs.

Verizon websites and services may include social network or other third-party plug-ins and widgets that may provide information to their associated social networks or third-parties about your interactions with Verizon page you visit or services you use, even if you do not click on or otherwise interact with the plug-in or widget. More information is available [here](#).

[Back to Summary](#)

How to Limit the Sharing and Use of Your Information

You have choices about how Verizon shares and uses information.

Customer Proprietary Network Information (CPNI):

As described [above](#), customers of Verizon telecommunication and VoIP services may choose whether to allow Verizon to share your CPNI within the Verizon family of companies for certain marketing purposes. This choice will remain in effect unless you change it. Verizon Wireline consumer and small business customers may opt-out of this sharing by calling us using the [state toll-free number provided in their notice and available here](#). Verizon Wireless mass-market customers may call 1-800-333-9956. National and major account customers of Verizon Wireless and corporate and government customers of Verizon Wireless or Verizon Business in the United States may decline to provide or withdraw CPNI consent by following the instructions in your service agreements or CPNI consent forms.

Telemarketing:

Federal "Do Not Call" laws allow you to place your phone numbers on the National Do Not Call Registry to prevent telemarketing calls to those numbers. If you would like to add your numbers to this list, you may do so by calling 1-888-382-1222, or by visiting www.donotcall.gov.

You should be aware that even if you add your number(s) to the federal or a state Do Not Call list, most telemarketing laws allow companies to contact their own customers. If at any time you would like to be removed from Verizon's residential telemarketing list, please let us know by contacting a Verizon customer service representative at 1-800-VERIZON.

Verizon Wireless also maintains a Do Not Call list. If you would like to be removed from the Verizon Wireless telemarketing list, please let us know by contacting a Verizon Wireless customer service representative at 1-800-922-0204. Please allow 30 days for your telephone number to be removed from any sales programs that are currently underway.


Marketing Email, Text Messages, Postal Mail and Door-to-Door Calls:

Marketing emails you receive from Verizon, Verizon Wireless, or Redbox Instant by Verizon include an unsubscribe instruction (usually found at the bottom of the email) that you may use to opt out of receiving future marketing-related emails. You may opt out of receiving marketing-related emails from Verizon by visiting our "Unsubscribe" site and providing the requested information. You may opt out of receiving marketing-related emails from Verizon Wireless by contacting a Verizon Wireless customer service representative at 1-800-922-0204. You may opt-out of receiving marketing-related emails from Redbox Instant by Verizon at your customer account pages [online](#).

You may opt out of receiving marketing-related postal mailings or prevent door-to-door marketing solicitations from Verizon by calling a customer service representative at 1-800-VERIZON. You may opt out of receiving marketing-related postal mailing or prevent text message marketing by Verizon Wireless by calling a Verizon Wireless customer service representative at 1-800-922-0204. Text message solicitations from Verizon also contain an "unsubscribe" feature that you can use to prevent future marketing text messages from us. Please note that Verizon may use bulk mail service for some marketing mailings. These services deliver offers to all homes in a neighborhood or zip code. This type of mailing will continue even if you opt-out of receiving marketing-related postal mailings from Verizon.

Information Used for Online Advertising:

You have choices about whether certain information collected on websites, including Verizon's, is used to customize advertising based on predictions generated from your visits over

time and across different websites. When you see this icon  in or around an advertisement you can click on the icon to see additional information on the companies and data practices that were used to deliver the ad and descriptions of how you may opt-out of these advertising programs. To learn more or to limit the collection of information by these parties, you may also visit the [Aboutads info](#) website.

Please note that many opt-outs are cookie-based. If you buy a new computer, change web browsers or delete the cookies on your computer, you will need to opt-out again. Please also note that some wireless devices, portals and websites have limited ability to use and store cookies. As a result, advertising entities may have a limited ability to use cookies in the manner described above or to respect cookie-based opt out preferences. However, ads may still be tailored using other techniques such as publisher, device or browser-enabled targeting. You should check the privacy policies of the products, sites and services you use to learn more about any such techniques and your options. If you do not want information to be collected for marketing purposes from services such as the Verizon Wireless Mobile Internet services, you should not use those particular services.

You also can limit the collection of certain website information by deleting or disabling cookies. Most computers' Internet browsers enable you to erase cookies from your computer hard drive, block all cookies, or receive a warning before a cookie is stored.

[See information about managing cookies](#)

Please note that disabling cookies may prevent you from using specific features on our sites and other websites, such as ordering products or services and maintaining an online account. Cookies must be enabled for you to use your Verizon e-mail account.

Relevant Advertising

Verizon broadband Internet access customers may opt-out of the relevant online advertising program described above by following the instructions [here](#). Verizon Wireless Internet customers may opt-out of the relevant mobile advertising program by following the instructions [here](#) or by calling us at 1-866-211-0874. You may opt-out of Verizon's Relevant TV advertising program by following the instructions [here](#). If you opt out online, you will need your account user ID and password. Also, please note that you will receive ads whether you participate in these programs or not, but under these programs, ads may be more relevant to you.

Business and Marketing Reports

Verizon Wireless customers may choose not to participate in Verizon Wireless' use of their information to create aggregated [business and marketing reports](#) that do not specifically identify any individual Verizon Wireless customers. You may opt-out by calling 1-866-211-0874 or by visiting verizonwireless.com/myprivacy. Please note that if you have a Family SharePlan® or multi-line account, you must indicate your opt-out choice for each line. If you add a line or change a telephone number, you will need to update your privacy choices.

[Back to Summary](#)

Working Together to Keep Children Safe

Verizon recognizes that online service providers must be vigilant in protecting the safety and privacy of children online. We do not knowingly market to or solicit information from children under the age of 13, without obtaining verifiable parental consent.

Verizon strongly supports educating parents and young internet users on safe viewing practices and we offer a variety of tools to help children and parents avoid encountering objectionable content or communications while using our services.

Verizon's [Parental Control Center](#) provides many free resources that offer guidance, connect parents with experts and help give parents the technical knowledge to help keep kids safer online.

Regrettably, there are those who use the Internet to view, store and distribute child pornography (or who engage in other types of illegal activity involving children). Child pornography is subject to severe criminal penalties and using the Verizon network to view, store or distribute it violates our service contracts. The Verizon network may not be used by customers in any manner for the storage, transmission or dissemination of images containing child pornography and we will report any instances of such activity of which we become aware to the appropriate law enforcement authorities.

If you have a complaint about child pornography, the soliciting of children for sexual activity, or any other illegal or inappropriate activity involving children on a Verizon service, report it to us by sending an email to abuse@verizon.net. Please include the words "child porn" in the subject line of your email. You can also make a report directly to the National Center for Missing and Exploited Children through its CyberTipline located at www.cybertipline.org.

Additional Internet safety resources and information are available at:

<http://www.netsmartz.org/>
<http://www.wiredsafety.org/>
<http://www.onguardonline.gov/>
<http://www.commonssensemedia.org/>
<http://www.stopbullying.gov/>
<http://www.cyberbullying.us/>
<http://www.connectsafely.org/>

[Back to Summary](#)

Information Security and Data Retention

Verizon has technical, administrative and physical safeguards in place to help protect against unauthorized access to, use or disclosure of customer information we collect or store, including Social Security Numbers. Employees are trained on the importance of protecting privacy and on the proper access to, use and disclosure of customer information. Under our practices and policies, access to sensitive personally identifiable information is authorized only for those who have a business need for such access. Personally identifiable and other sensitive records are retained only as long as reasonably necessary for business accounting, tax or legal purposes.

Although we work hard to protect personal information that we collect and store, no program is 100% secure and we cannot guarantee that our safeguards will prevent every unauthorized attempt to access, use or disclose personal information. Verizon maintains security and incident response plans to handle incidents involving unauthorized access to private information we collect or store.

If you become aware of a security issue, please contact [Verizon's Security Control Center](#). We will work with you to address any problems.

Verizon often publishes helpful information about a wide range of scams that you may encounter.

[View current information about Internet and phone scams and tips on how to protect yourself](#)

[Back to Summary](#)

Contact Information

If you have questions, concerns or suggestions related to our Privacy Policy or our privacy practices you may contact us at:

Verizon Privacy Office
1300 I Street, NW
Suite 400 West
Washington, DC 20005
Fax: 202-789-1432
Email: privacyoffice@verizon.com

Accessing and Updating Your Information

We strive to keep our customer records as accurate as possible. You may correct or update your Verizon customer information by calling a Verizon customer service representative at 1-800-VERIZON or by accessing your account online and providing the updated information there. Similarly, updates can be made to your Verizon Wireless account by calling a Verizon Wireless customer service representative at 1-800-922-0204 or [online](#). Verizon Business customers may update their information by contacting their account manager. Updates can be made to your Redbox Instant by Verizon account information by visiting the "My Account" pages [online](#).

If you are a FIOS or other customer served over our fiber-to-the-premises network and you would like to see your personally identifiable information, please contact us at privacyoffice@verizon.com so we may arrange a time and convenient location for you to do so during business hours. You will need to provide proper identification and you may examine records that contain personally identifiable information about you and no one else. If you believe any of your personally identifiable information is inaccurate, we will work with you to ensure that corrections are made. Verizon reserves the right to charge you for the cost of photocopying any documents you request.

Links to and from non-Verizon Websites and Content

Verizon websites and Redbox Instant by Verizon platforms may contain links to non-Verizon sites. Verizon applications or other content may be included on web pages and web sites that are not associated with Verizon and over which we have no control. We are not responsible for the content on these sites or platforms or the privacy policies and practices employed by these sites and platforms. We recommend that you review the policies and practices of the sites you visit.

Information Sharing: Blogs and Social Networking

Some Verizon websites, applications, and services may allow you to participate in web log ("blog") discussions, message boards, chat rooms, and other forms of social networking and to post reviews. Please be aware that these forums are accessible to others. We urge you to not submit any personally identifiable information to these forums because any information you post can be read, collected, shared, or otherwise used by anyone who accesses the forum. Verizon is not responsible for the information you choose to submit in these forums. If you post content to information sharing forums, including any information about the movies you rent or view, you are doing so by choice and you are providing consent to the disclosure of this information.

Changes to This Policy

We reserve the right to make changes to this Privacy Policy, so please check back periodically for changes. You will be able to see that changes have been made by checking to see the effective date posted at the end of the policy.

If Verizon elects to use or disclose information that identifies you as an individual in a manner that is materially different from that stated in our policy at the time we collected that information from you, we will give you a choice regarding such use or disclosure by appropriate means, which may include use of an opt-out mechanism.

Updated January 2014

© 2009, 2011-2014 Verizon. All Rights Reserved.



Verizon Transparency Report

U.S. Data

In 2013, Verizon received approximately 320,000 requests for customer information from federal, state or local law enforcement in the United States. We do not release customer information unless authorized by law, such as a valid law enforcement demand or an appropriate request in an emergency involving the danger of death or serious physical injury.

The table below sets out the number of subpoenas, orders, and warrants we received from law enforcement in the United States last year. We also received emergency requests and National Security Letters. The vast majority of these various types of demands relate to our consumer customers; we receive relatively few demands regarding our enterprise customers.

Overall, we saw an increase in the number of demands we received in 2013, as compared to 2012.

Law Enforcement Demands for Customer Data — United States (2013)

Subpoenas 164,184

Orders 70,665

62,857 General Orders

6,312 Pen Registers/ Trap & Trace Orders

1,496 Wiretap Orders

Warrants 36,696

Emergency Requests From Law Enforcement 50,000 (approximately)

Total 321,545

National Security Letters 1000-1999

Which Verizon services does this Transparency Report cover?

The figures in this Report include demands for customer data regarding our Verizon wireline services, such as phone, Internet or television, and our Verizon Wireless services.

Does this Transparency Report include information on the number of national security orders you receive?

Like all other companies to issue transparency reports, we are not permitted at this time to report information on national security orders (like FISA orders). We do report, within a range, the number of National Security Letters that we received from the FBI in 2013; we report only a range because, like the other companies that have published transparency reports, we have not been granted permission to indicate the exact number of National Security Letters we received. Last week, President Obama announced that telecommunications providers will be permitted to make public more information in the future; we encourage greater transparency and, if permitted, will make those additional disclosures.

Does Verizon reject law enforcement demands?

Yes. If a demand is facially invalid, or if a demand seeks certain information that can only be obtained with a different form of process (for example, a subpoena, rather than a warrant, improperly is used to seek stored customer content), we reject the demand. If a demand is overly broad or vague we will not produce any information, or will seek to narrow the scope of the demand and produce a subset of the information sought. In many cases we do not produce any information at all, including because the demand seeks information we do not have.

Is Verizon reporting on the percentage of demands for which it did not produce any data?

We did not track the percentage of demands to which we produced some or no data in 2013, but will be doing so going forward. As just noted, we carefully review each demand and reject in whole or part those that are deficient.

Does Verizon charge law enforcement for providing data?

In some instances, Federal and most state laws authorize providers to charge a reimbursement fee for responding to law enforcement demands for records or to recoup reasonable expenses in complying with a wiretap order or pen register or trap and trace order. In the majority of instances, however, we do not seek reimbursement for responding to law enforcement requests. We do not charge for responding to emergency requests and do not charge for responding to most subpoenas. When we do charge a reimbursement fee, our fees are permitted by law or court order and seek to recoup only some of our costs.

Does Verizon also receive requests for data in civil cases?

Yes, we do. Requests in civil cases comprise a small percentage of the total requests we receive. This report focuses on requests from law enforcement.

Will Verizon issue future transparency reports?

Yes, on a semi-annual basis.

What obligations to report on demands already apply to the United States government?

Federal law already places substantial reporting requirements on federal and state governments.

Each year the United States Attorney General and the principal prosecuting attorney for each state have to report the number of applications for wiretap orders, the number of orders granted, the types of communications intercepted, the number of persons whose communications were intercepted and the numbers of arrests and convictions resulting from such interceptions. That information is summarized for Congress. See 18 U.S.C. § 2519(2),(3). Similarly, the Attorney General must make detailed annual reports to Congress on the number of pen registers and trap and trace orders. See 18 U.S.C. § 3126.

The Attorney General also has to report to Congress each year regarding information obtained in emergencies, in some contexts. See 18 U.S.C. § 2702(d). And the Director of the FBI has to report twice each year to Congress regarding the number of National Security Letters issued. See 18 U.S.C. § 2709(e).

Subpoenas

We received approximately 164,000 subpoenas from law enforcement in the United States last year. We are required by law to provide the information requested in a valid subpoena. The subpoenas we receive are generally used by law enforcement to obtain subscriber information or the type of information that appears on a customer's phone bill. More than half of the subpoenas we receive seek only subscriber information: that is, those subpoenas typically require us to provide the name and address of a customer assigned a given phone number or IP address. Other subpoenas also ask for certain transactional information, such as phone numbers that a customer called. The types of information we can provide in response to a subpoena are limited by law. We do not release contents of communications (such as text messages or emails) or cell site location information in response to subpoenas.

Does a law enforcement officer need to go before a judge to issue a subpoena?

Under federal law and the law in many states the government does not need judicial approval to issue a subpoena. A prosecutor or law enforcement official may issue a subpoena to seek evidence relevant to the investigation of a possible crime.

Are there limits on the types of data law enforcement can obtain through a subpoena?

Yes, in response to a subpoena, we only release the six types of information specifically identified in section 2703(c)(2)(A)-(F) of Title 18 of the United States Code: customer name, address, telephone or other subscriber number, length of service, calling records and payment records. Some states have stricter rules. We do not release any content of a communication in response to a subpoena.

Are there different types of subpoenas?

Yes, we may receive three different types of subpoenas from law enforcement: a grand jury subpoena (the subpoena is issued in the name of a grand jury investigating a potential crime); an administrative subpoena (generally, a federal or state law authorizes a law enforcement agency to issue a subpoena); or a trial subpoena (the subpoena is issued in the name of the court in anticipation of a trial or hearing).

Orders

We received about 70,000 court orders last year. These court orders must be signed by a judge, indicating that the law enforcement officer has made the requisite showing required under the law to the judge. The orders compel us to provide some type of information to the government.

General Orders. Most of the orders we received last year – almost 63,000 – were “general orders.” We use the term “general order” to refer to an order other than a wiretap order, warrant, or pen register or trap and trace order. Almost half of the general orders required us to release the same types of basic information that could also be released pursuant to a subpoena. We do not provide law enforcement any stored content (such as text messages or email) in response to a general order.

“Pen/Trap” Orders and Wiretap Orders. A small subset of the orders we received last year – about 7,800 – required us to provide access to data in real-time. A pen register order requires us to provide law enforcement with real-time access to phone numbers as they are dialed, while a trap and trace order compels us to provide law enforcement with real-time access to the phone numbers from incoming calls. We do not provide any content in response to pen register or trap and trace orders. We received about 6,300 court orders to assist with pen registers or trap and traces last year, although generally a single order is for both a pen register and trap and trace. Far less frequently, we are required to assist with wiretaps, where law enforcement accesses the content of a communication as it is taking place. We received about 1,500 wiretap orders last year.

What is a pen register or trap and trace order?

Pen register or trap and trace orders require a wire or electronic communications provider (like Verizon) to afford access to “dialing, routing, addressing or signaling information.” With a pen register order we must afford real-time access to the numbers that a customer dials (or IP addresses that a customer visits); with a trap and trace order we must afford real-time access to the numbers that call a customer. Such orders do not authorize law enforcement to obtain the contents of any communication.

What is a wiretap order?

A wiretap order is an order that requires a wire or electronic communications provider to provide access to the content of communications in real-time to law enforcement. The order can relate to the content of telephone or Internet communications.

What are the different showings that law enforcement has to make for the different orders?

A wiretap order is the most difficult for law enforcement to obtain. Under the law, law enforcement may not obtain a wiretap order unless a judge finds that there is probable cause to believe that an individual is committing one of certain specified offenses and that particular communications concerning that offense will be obtained through the wiretap. A wiretap order is only issued for a specified time.

A general order requires law enforcement to offer specific and articulable facts showing that there are reasonable grounds to believe that the records sought are relevant and material to an ongoing criminal investigation. In federal court, such orders are authorized under 18 U.S.C. § 2703(d).

A pen register order or trap and trace order requires law enforcement to make a lesser showing -- that the information likely to be obtained is relevant to an ongoing criminal investigation.

Warrants

We received about 36,000 warrants last year. To obtain a warrant a law enforcement officer must show a judge that there is "probable cause" to believe that the evidence sought is related to a crime. This is a higher standard than the standard for a general order. While many warrants seek the same types of information that can also be obtained through a general order or subpoena, most warrants we received in 2013 sought stored content or location information.

What showing must law enforcement make to obtain a warrant?

To obtain a warrant a law enforcement officer has to show a judge that there is probable cause to believe that the evidence it seeks is related to a crime and in the specific place to be searched.

What is the difference between stored content and non-content?

"Stored content" refers to communications or other data that our users create and store through our services, such as text messages, email or photographs. We require a warrant before disclosing stored content to law enforcement, absent an emergency involving the danger of death or serious physical injury. Non-content refers to records we create such as subscriber information that a customer provides at the time she signs-up for our services, and transactional information regarding the customer's use of our services, such as phone numbers that a customer called.

Content and Location Information

Content. We are compelled to provide contents of communications to law enforcement relatively infrequently. Under the law, law enforcement may seek communications or other content that a customer may store through our services, such as text messages or email. Verizon only releases such stored content to law enforcement with a warrant; we do not produce stored content in response to a general order or subpoena. Last year, we received approximately 14,500 warrants for stored content.

As explained above, law enforcement may also present a wiretap order to obtain access to the content of a communication as it is taking place, which they did about 1,500 times last year. Taken together, the number of orders for stored content and to wiretap content in real-time accounted for only about five percent of the total number of demands we received in 2013.

Location Information. Verizon only produces location information in response to a warrant or order; we do not produce location information in response to a subpoena. Last year, we received about 35,000 demands for location data: about 24,000 of those were through orders and about 11,000 through warrants. In addition, we received about 3,200 warrants or court orders for “cell tower dumps” last year. In such instances, the warrant or court order compelled us to identify the phone numbers of all phones that connected to a specific cell tower during a given period of time. The number of warrants and orders for location information are increasing each year.

Emergency Requests

Law enforcement requests information from Verizon that is needed to help resolve serious emergencies. We are authorized by federal law to provide the requested information in such emergencies and we have an established process to respond to emergency requests, in accordance with the law. To request data during these emergencies, a law enforcement officer must certify in writing that there was an emergency involving the danger of death or serious physical injury to a person that required disclosure without delay. These emergency requests are made in response to active violent crimes, bomb threats, hostage situations, kidnappings and fugitive scenarios, often presenting life-threatening situations. In addition, many emergency requests are in search and rescue settings or when law enforcement is trying to locate a missing child or elderly person.

We also receive emergency requests for information from Public Safety Answering Points regarding particular 9-1-1 calls from the public. Calls for emergency services, such as police, fire or ambulance, are answered in call centers throughout the country, known as PSAPs. PSAPs receive tens of millions of calls from 9-1-1 callers each year, and certain information about the calls (name and address for wireline callers; phone numbers and available location information for wireless callers) is typically made available to the PSAP when a 9-1-1 call is made. Yet a small percentage of the time PSAP officials need to contact the telecom provider to get information that was not automatically communicated by virtue of the 9-1-1 call or by the 9-1-1 caller.

In 2013, we received 85,116 emergency requests for information from law enforcement in emergency matters involving the danger of death or serious physical injury or from PSAPs relating to particular 9-1-1 calls from the public for emergency services. While in 2013 we did not track whether an emergency request was made by law enforcement or PSAPs, we are doing so now. We estimate that at least half of these requests – approximately 50,000 – were from law enforcement pursuant to the emergency procedures discussed above and the remainder were from PSAPs after receiving 9-1-1 calls from the public.

National Security Letters

We also received between 1,000 and 2,000 National Security Letters in 2013. We are not permitted to disclose the exact number of National Security Letters that were issued to us, but the government will allow us to provide a broad range.

What is an NSL?

A National Security Letter, or NSL, is a request for information in national security matters; it cannot be used in ordinary criminal, civil or administrative matters. When the Director of the Federal Bureau of Investigation issues a National Security Letter to a wire or electronic communications provider (like Verizon) such a provider must comply. The law that authorizes the FBI to issue NSLs also requires the Director of the FBI to report to Congress regarding NSL requests.

Under what circumstances can the FBI issue an NSL?

The FBI does not need to go to court to issue an NSL. Rather, the Director of the FBI or a senior designee must certify in writing that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.

What types of data can the FBI obtain through an NSL?

The FBI may seek only limited categories of information through an NSL: name, address, length of service and toll billing records. The FBI cannot obtain other information from Verizon, such as content or location information, through an NSL.

Does this Transparency Report include information on the number of national security orders you receive?

We report only information about National Security Letters. Like all other companies to issue transparency reports, we are not permitted at this time to report information on national security orders (like FISA orders).

Verizon Transparency Report

International Data

This table shows the total number of demands for customer information made by law enforcement to Verizon in 2013 in every country in which we do business, and had any such demands, other than the United States. While we offer services to business, government and consumer customers in the United States, our focus outside the United States is on business and enterprise customers. Only countries from which we received demands in 2013 are included in this chart. As explained below, there are some limits to what we can disclose regarding law enforcement demands.

These figures reflect requests made by law enforcement within a country for data stored within that same country. It is very rare that we receive a request from a government for data stored in another country. When this occurs, it generally is a request for United States consumer data from a government entity outside the United States; when we receive these infrequent requests, we do not comply and instead direct the requesting government agency to make its request through any applicable diplomatic channels (like the Mutual Legal Assistance Treaty process) in its country. In 2013, we did not receive any demands from the United States government for data stored in other countries. We received a small number of requests last year from non-U.S. governments for data stored in the United States, all of which were referred to the MLAT process.

On occasion, we are required by government orders, regulations or other legal requirements to block access to specified websites outside the United States. While we have not received such blocking demands in the United States, we did receive such demands in five countries in 2013. In Colombia, we were required to block access to approximately 1,200 websites that the Colombian government believed contained child pornography. In Greece, we were required to block 424 sites related to online gambling. We were also required to block websites in Belgium (37) and Portugal (2) related to online gambling or copyright issues. Finally, we were required to block access to websites in India but are precluded by law from identifying the specific number of websites. (These figures relate to the number of websites we were required to block access to in 2013. We may be required to block access to such websites for an ongoing period of time, but we count such demands only for the year in which they were initially made.)

Law Enforcement Demands for Data (Outside of the United States - 2013)

Australia	29
Austria	8
Belgium	473
France	1,347
Germany	2,996
Italy	13
Japan	14
Netherlands	65

Switzerland	60
Taiwan	1
UK	386

Is this International Report impacted by countries that do not allow Verizon to report certain data?

Yes, the laws in some countries, such as Australia and India, limit what we can disclose. In Australia we are precluded by law from reporting the number of warrants we received from law enforcement for interceptions or stored communications. And, in India we are precluded by law from discussing any information about the requests we might receive from the Government of India or identifying the specific number of websites that we were asked to block by the Government of India.

Verizon Transparency Report

National Security

The table below sets forth the number of national security demands we received in 2013. We note that while we now are able to provide more information about national security orders that directly relate to our customers, reporting on other matters, such as any orders we may have received related to the bulk collection of non-content information, remains prohibited.

National Security Demands

	Jan. 1, 2013 – June 30, 2013	July 1, 2013 – Dec. 31, 2013
National Security Letters	0-999	0-999
Number of customer selectors	2000-2999	2000-2999
FISA Orders (Content)	0-999	*
Number of customer selectors	4000-4999	*
FISA Orders (Non-Content)	0-999	*
Number of customer selectors	0-999	*

* The government has imposed a six month delay for reporting this data

National Security Letters

We explained in our Transparency Report that we had received between 1000 and 1999 National Security Letters in 2013. We separately provide details for the first half and second half of 2013 now; in the future, we will make semi-annual reports regarding only the immediately preceding six month period. In the first half of 2013, we received between 0 and 999 NSLs from the FBI. Similarly, we received between 0 and 999 NSLs in the second part of 2013. In the first six months of the year, those NSLs sought information regarding between 2000 and 2999 “selectors” used to identify a Verizon customer. The same is true for the second half of 2013. (The government uses the term “customer selector” to refer to an identifier, most often a phone number, which specifies a customer. The number of selectors is generally greater than the number of “customer accounts.” An NSL might ask for the names associated with two different telephone numbers; even if both phone numbers were assigned to the same customer account, we would count them as two selectors.)

As we explained in our Transparency Report, the FBI may seek only limited categories of information through an NSL: name, address, length of service and toll billing records. Verizon does not release any other information in response to an NSL, such as content or location information.

FISA orders

The government requires that we delay the report of any orders issued under the Foreign Intelligence Surveillance Act for six months. Thus, at this time, we may report FISA information only for the first half of 2013. In July, or soon thereafter, we will report FISA information regarding the second half of 2013.

Content

From January 1, 2013 through June 30, 2013, we received between 0 and 999 FISA orders for content. Those orders targeted between 4000 and 4999 "customer selectors" used to identify a Verizon customer.

Non-Content

From January 1, 2013 through June 30, 2013, we received between 0 and 999 reportable FISA orders for non-content. Some FISA orders that seek content also seek non-content; we counted those as FISA orders for content and to avoid double counting have not also counted them as FISA orders for non-content. Those orders targeted between 0 and 999 "customer selectors."

We will update our Transparency Report again in the middle of the year.