DESCRIPTION OF 2013 RAA DATA RETENTION SPECIFICATION DATA ELEMENTS
AND POTENTIALLY LEGITIMATE PURPOSES FOR COLLECTION/RETENTION
DISCUSSION DRAFT ONLY 21 March 2014

Data Element	**Explanation of Data Element**	**Potentially Legitimate purposes for Collection/Retention**
1.1.1. First and last name or full legal name of Registrant	Self evident	Registrar's internal use for administration of the contract with Registrant both during and for some period of time after the registration (to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP) Billing Billing disputes Chargebacks
1.1.2. First and last name or, in the event Registrant is a legal person, the title of the Registrant's administrative contact, technical contact, and billing contact	Self evident	Registrar's internal use for administration of the contract with Registrant both during and for some period of time after the registration (to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP) Billing Billing disputes Chargebacks
1.1.3. Postal address of Registrant, administrative contact, technical contact, and billing contact	Self evident	Registrar's internal use for administration of the contract with Registrant both during and for some period of time after the registration (to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP) Billing Billing disputes Chargebacks
1.1.4. Email address of Registrant, administrative contact, technical contact, and billing contact;	Self evident	Registrar's internal use for administration of the contract with Registrant both during and for some period of time after the registration (to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP) Billing Billing disputes Chargebacks

DESCRIPTION OF 2013 RAA DATA RETENTION SPECIFICATION DATA ELEMENTS
AND POTENTIALLY LEGITIMATE PURPOSES FOR COLLECTION/RETENTION
DISCUSSION DRAFT ONLY 21 March 2014

Data Element	**Explanation of Data Element**	**Potentially Legitimate purposes for Collection/Retention**
1.1.5. Telephone contact for Registrant, administrative contact, technical contact, and billing contact;	Self evident	Registrar's internal use for administration of the contract with Registrant both during and for some period of time after the registration (to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP) Billing Billing disputes Chargebacks
1.1.6. WHOIS information, as set forth in the WHOIS Specification	Self evident	Data Enabling Registrar to populate and make available to the public community the WHOIS register both during and for some period of time after the registration (to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP) Abuse mitigation Facilitating domain name purchases and sales
1.1.7. Types of domain name services purchased for use in connection with the Registration;	Self evident	Registrar's internal use for administration of the contract with Registrant both during and for some period of time after the registration (to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP) Billing Billing disputes Chargebacks

DESCRIPTION OF 2013 RAA DATA RETENTION SPECIFICATION DATA ELEMENTS
AND POTENTIALLY LEGITIMATE PURPOSES FOR COLLECTION/RETENTION
DISCUSSION DRAFT ONLY 21 March 2014

Data Element	**Explanation of Data Element**	**Potentially Legitimate Purposes for Collection/Retention**
1.1.8. To the extent collected by Registrar, "card on file," current period third party transaction number, or other recurring payment data	Section 1.1.8 focuses on data required for processing of recurring payments. Some (not all) Registrants provide Registrars with credit card numbers to retain as a "card on file," or with bank account information so that recurring payments such as monthly fees or automatic renewals can be billed periodically. The information retained would include whatever is required for the credit card company to process the recurring payment transaction (typically credit card number, expiration date, name on card, address or postal code, sometimes security code). Alternatively, a Registrant might authorize recurring payments to be made by automatically debiting the Registrant's bank account via an automated clearing house (ACH) bank debit, which would require storing the account holder's name, bank routing number and bank account number. Whether recurring payments are authorized to be charged by credit card or by bank debit, any recurring payment mechanism and associated retention of recurring payment information would require the Registrant's authorization to retain such information for recurring payments. When the Registrar submits a credit card transaction for processing of any payment, an authorization will generate an approval code, which the Registrar stores with the transaction. Banks or financial institutions may generate and provide to the Registrar a bank-generated transaction ID number for each payment made.	Registrar's internal use for administration of the contract with Registrant both during and for some period of time after the registration (to address hijacking, slamming and to facilitate resolution of transfer disputes in accordance with th TDRP) Billing Billing disputes Chargebacks

DESCRIPTION OF 2013 RAA DATA RETENTION SPECIFICATION DATA ELEMENTS
AND POTENTIALLY LEGITIMATE PURPOSES FOR COLLECTION/RETENTION
DISCUSSION DRAFT ONLY 21 March 2014

Data Element	**Explanation of Data Element**	**Potentially Legitimate Purposes for Collection/Retention**
1.2.1. Information regarding the means and source of payment reasonably necessary for the Registrar to process the Registration transaction, or a transaction number provided by a third party payment processor	Section 1.2.1 focuses on source of payment information required for processing of the initial Registration transaction (without regard to whether recurring payments are authorized). The data would be similar to that in Section 1.1.8 above (which deals with recurring payments). Banks or financial institutions may generate and provide to the Registrar a bank-generated transaction ID number for each payment made.	Registrar's internal use for administration of the contract with Registrant both during and for some period of time after the registration Maintain Registrar's tax and accounting records Billing Billing disputes Fraud prevention Chargebacks

DESCRIPTION OF 2013 RAA DATA RETENTION SPECIFICATION DATA ELEMENTS
AND POTENTIALLY LEGITIMATE PURPOSES FOR COLLECTION/RETENTION
DISCUSSION DRAFT ONLY 21 March 2014

Data Element	**Explanation of Data Element**	**Potentially Legitimate Purposes for Collection/Retention**
1.2.2. Log files, billing records and, to the extent collection and maintenance of such records is commercially practicable or consistent with industry-wide generally accepted standard practices within the industries in which Registrar operates, other records containing communications source and destination information, including, depending on the method of transmission and without limitation: (1) Source IP address, HTTP headers, (2) the telephone, text, or fax number; and (3) email address, Skype handle, or instant messaging identifier, associated with communications between Registrar and the Registrant about the Registration	Section 1.2.2 focuses on records associated with communications between Registrar and the Registrant about the Registration with an emphasis on information regarding the source and destination of the communications. Most commercially available server software gathers certain information regarding website visits automatically and stores it in log files. This information typically consists of an Internet Protocol (IP) address that consists at a minimum of a series of numbers, as well as browser type, internet service provider (ISP), referring/exit pages, operating system, date/time stamp; this type of data is typically not linked to personally identifiable information and is used for aggregate analysis. In addition to this non-personally-identifiable data, some log files may include data identifying the source of the communication (IP address, telephone/text/fax number, email address or Skype handle or instant messaging identifier). In some cases that information may be linked to data about the particular user's behavior while on the website, including what the user has put in or taken out of their shopping cart, and what items the user purchases. The latter type of log file data may be important in the event of billing disputes or fraud, e.g., to show that the Registrant or someone using the Registrant's email address or IP address did in fact place a disputed order on a particular date at a particular time.	Fraud prevention Billing disputes Resolution of disputes between Registrar and Registry Operator or between two Registrars or between Registrar and Registrant regarding the status of a Registration, e.g., Registrant says it never authorized the transfer of a domain name from one Registrar to another Registrar; log files maintained by Registrar could show when and from what source a request for transfer was made.

DESCRIPTION OF 2013 RAA DATA RETENTION SPECIFICATION DATA ELEMENTS
AND POTENTIALLY LEGITIMATE PURPOSES FOR COLLECTION/RETENTION
DISCUSSION DRAFT ONLY 21 March 2014

Data Element	**Explanation of Data Element**	**Potentially Legitimate Purposes for Collection/Retention**
1.2.3. Log files and, to the extent collection and maintenance of such records is commercially practicable or consistent with industry-wide generally accepted standard practices within the industries in which Registrar operates, other records associated with the Registration containing dates, times, and time zones of communications and sessions, including initial registration	Section 1.2.3 focuses on records associated with the Registration. This may include communications with the Registrant regarding the Registration (see Section 1.2.2 above), but may also include records of communications between the Registrar and the Registry Operator about the Registration. Most Registrars and Registry Operators utilize the Extensible Provisioning Protocol (EPP) protocol to track, manage and reconcile the status of domain name registrations (e.g., statuses such as register, renew, modify, delete, transfer). Software used by Registrars and Registry Operators often maintain log files tracking EPP records such as when a Registration is first made, when it is transferred or deleted, when it is modified, etc. and assign unique authorization codes to events as a security measure to prevent unauthorized transfers, deletions or other abuse. Typical web server software can be configured to maintain html server logs, stored either on the Registrar's server or in cookies on the Registrant's browser or both, either in encrypted or unencrypted form, and with the option of allowing the user (the Registrant) to allow or prevent storage in the form of cookies in its browser.	Fraud prevention Billing disputes Resolution of disputes between Registrar and Registry Operator or between two Registrars or between Registrar and Registrant regarding the status of a Registration (e.g., Registrant says it never authorized the transfer of a domain name from one Registrar to another Registrar; log files maintained by Registrar could show when and from what source a request for transfer was made and if or when Registrar transmitted to the Registry Operator a request to transfer the registration.

EXPLANATION OF POTENTIALLY LEGITIMATE PURPOSES
DISCUSSION DRAFT ONLY 21 March 2014

Registrar's internal use for administration of the contract with Registrant	Administration of the contract during the life of the registration and for some period of time thereafter. During the registration period, a Registrar would require details of the person or legal entity that has made the registration (i.e. full name if a living person) and details of appropriate points of contact to address administrative, technical and billing contacts, for purposes of contacting the Registrant to address matters such as contract extension or renewal, billing, promotional offers, etc. This purpose would also require the Registrar to retain this data for a reasonable period after expiry of the registration to allow for renewal. By way of example, many registries offer a 45-day grace period for the Registrant to renew. If the domain name is not renewed, there is a further 30-day grace period during which the Registrant could still claim the domain name.
Tax and accounting records	Records of billings and payments may be required to substantiate the Registrar's accounting and tax records
Fraud prevention	Retaining records of communications and/or log files showing dates and times of interactions and source of communications may be necessary to avoid fraud, e.g., a fraudulent claim by a Registrant that it did not order a particular product or service or did not authorize a change to existing services ordered
Billing disputes and chargebacks	If all records of transactions, source of payment information, etc. are deleted, a Registrar will have no way to evaluate billing dispute claims or process chargebacks. In many cases disputed credit card or bank charges may not be noticed for a year or more, and requests for chargebacks, refunds or credits a year or more after the charge are not uncommon
Billing	Data necessary to bill and collect amounts owned from the Registrant
Abuse mitigation	Private parties who are targets of spam, phishing, malware, fraud and similar abuses can often identify the website that is the source of the activity. Sometimes the owner of the website or domain name is unaware that its side has been compromised and is being used to enable these activities. Access to WHOIS data assists private parties in contacting the owner of the domain from which these activities originate and working to remediate the problems.
Facilitating domain name purchases and sales	If someone wishes to purchase an existing domain name, access to WHOIS data allows a potential buyer to know who owns the name, when the registration expires, and how to contact that person to negotiate a potential purchase.

Hijacking, theft, slamming, TDRP	Protecting the Registrant against and providing remedies for domain name hijacking or theft. Domain names can be hijacked, i.e., transferred to another Registrant without authorization in several ways, including, for example, an unauthorized person hacking into the Registrant's computer or otherwise obtaining sufficient personal information and passwords to allow the unauthorized person to sign into the Registrant's account and transfer the domain name. A similar variation, sometimes referred to as domain slamming, occurs when a Registrant receives a fraudulent or deceptive letter, fax, phone call or email purporting to be from the Registrar that appears to be a domain name registration renewal. If the Registrant does not realize the communication is fraudulent, the Registrar may unknowingly transfer the registration to another Registrar. Another variation is that someone who obtains personal information and passwords may sign onto the Registrant's domain name account and terminate the registration. In all of these scenarios, if all data about a Registrant is automatically deleted immediately upon a transfer of the domain name to another Registrar or upon deletion of the domain name account, the Registrant may have no way of proving that it was the lawful owner of the domain and that the time was wrongfully transferred or deleted. Thus, the collection of data from the Registrant, and the retention of that data by the Registrar for a reasonable period of time after the registration terminates or is transferred, serves to protect the Registrant whose data was collected. A Transfer Dispute Resolution Policy (TDRP) is in place to resolve disputes between Registrars over alleged unauthorized transfers of domain names from one Registrar to another. A dispute must be filed no later than six (6) months after the alleged violation of the Transfer Policy. However, a Registrant may not always become aware of a domain name hijacking until after six months has expired. A crafty hijacker may change the registration of the domain name but leave the existing website in place for a period of time so it is not obvious to the Registrant that anything has changed, then transfer the registration again to a another Registrar, then potentially transfer the registration once again to yet another Registrar. By the time the Registrant becomes aware of the hijacking, a year or more may have elapsed and there may have been several intervening transfers of the registration. If the TDRP is not available to the Registrant because of the passage of time, the Registrant may be able to pursue judicial remedies, but would need the same information to prove its case. This suggests an appropriate period of retention is a year or more after the registration has been terminated or moved.

LAW ENFORCEMENT AND IP OWNER CONSIDERATIONS
DISCUSSION DRAFT ONLY 21 March 2014

A general note on law enforcement and IP owners: Although ICANN understands that these may not be recognized per se as legitimate purposes under the laws of some EU Member States, law enforcement and IP owners were strong advocates of the collection and retention of the information in the Data Retention Specification. This includes law enforcement officials from various EU Member States as well as Interpol. IP owners such as motion picture producers share these concerns. From the law enforcement perspective, consider a situation where an individual using hundreds of stolen credit cards sitting at an Internet cafe in Las Vegas purchases thousands of domain names, or that same individual hijacks hundreds of domain names. From a law enforcement perspective, being able to subpoena records that would include log files showing that all of these transactions originated from a single IP address that is traceable to a particular Internet cafe and that shows the dates and times the transactions occurred could be extremely valuable in finding the perpetrator. Similarly, if dozens of websites permitting downloading of pirated motion pictures can all be shown to have originated from orders placed via the same stolen credit cards and/or from the same IP address and/or in transactions that all originated at or near the same time, this may help copyright owners locate and pursue copyright infringers, either through civil or criminal enforcement. The views of privacy advocates from some government agencies are not necessarily aligned with the views of law enforcement and proprietary rights advocates from other agencies in the same jurisdiction. ICANN understands that if data is retained for legitimate purposes, law enforcement's ability to access such data will likely be determined under applicable local law, e.g., pursuant to a valid subpoena or court order.