|  |
| --- |
| Overarching Purpose: Digital Crime investigation by non-LEA  Terms:   * Secondary victim: a domain name registrant whose domain names, or resources hosted at that domain name, have been hijacked to deliver malware or act as bait in a phishing scam * Primary victim: an end user impacted by malware or phishing * Note: If the domain name registrant is engaged in criminal activity using the domain name, the concept of secondary victim would not apply. * Criminal infrastructure: a collection of servers and/or domain names used to perpetrate crimes, either as phishing bait, malware delivery systems, command and control nodes, or points of indirection. Criminal infrastructure may consist of elements hacked or stolen from victims and now under the control of the miscreant or may have been acquired lawfully by the miscreant and put to bad use. |

|  |  |
| --- | --- |
| Use Case: Initial investigation of criminal activity against a victim and/or secondary victim where domain names are used in the commission of the crime (part 1 of 2) | |
| 1. User Groups (Requestors) / User characteristics | **Digital crime investigators (corporate or academic). Most investigations of this type start with corporate or academic investigators. LEA relies heavily on these researchers.** |
| 1. Why is non-public registration data necessary? | Non-public registration data is requested in order to ascertain if the domain belongs to a secondary victim of a crime or is part of criminal infrastructure involved in the crime and to identify further investigatory requirements. |
| 1. Data elements that may typically be disclosed[[1]](#footnote-1) | * If there is reason to believe that the domain name owner is a secondary victim (i.e. a server hosted on that domain name has been compromised in order to steal from primary victim(s), the phone and email contact elements for both registrant and tech contact should be disclosed to facilitate immediate outreach to the secondary victim. * If the domain name owner is indeed a secondary victim, it is likely that they will give consent to disclose all other non-public data to assist in the investigation. * If there is reason to believe that the domain name owner is not a secondary victim but is in fact a perpetrator against the primary victims, the full set of nonpublic data will be requested to facilitate further investigation and identification. |
| 1. Lawful basis of entity disclosing non-public registration data to the requestor | 6(1)(a)  6(1)(b)  6(1)(f) |
| 1. Supporting info to determine lawful basis for the requestor | * Although an argument might be made that both the primary and secondary victims are subject to threat to their vital interests, the lack of threat of physical harm to the data subject weakens this argument. Instead, we considered 6(1)(a) or 6(1)(b) in cases where the data subject or primary victim are customers or business partners of the researching entity.   + Examples of this would be student victims at an investigating university or end users of an online service whose company also performs such investigations. * Failing this, 6(1)(f) is proposed.   + Example of 6(1)(f) might include investigations by Microsoft into crimes impacting the users of a Microsoft product or service who have not given explicit consent and whose contracts or user agreements do not explicitly mention such support by Microsoft to investigate such crimes. * **We request that a working group provide further clarification whether there exists an applicable basis in cases where investigations involve users with no connection to the researcher (i.e. those not using a product or service of the investigators), and where the intent of investigation is to improve the trustworthiness (e.g. security, stability and resiliency) of the Internet in general.** |
| 1. Safeguards (requirements) Applicable to the Requestor | The requestor:   1. Must process data in compliance with data protection laws such as GDPR, including secure transmission; 2. Must provide representations about use of requested data which will be subject to auditing.   Additional items to be considered in the development of a code of conduct[[2]](#footnote-2):  Individuals or entities seeking accreditation as a member of this user group must also:   * Agree to only use the data for the legitimate and lawful purpose described above; * Only issue disclosure requests with respect to the trademark(s) where ownership is evidenced; * Agree to:   + the terms of service, in which the lawful use of data described;   + prevent abuse of data received;   + be subject to de-accreditation if they are found to abuse use of data;   + maintain a register of all requests also including the respective rightsholders name (subject to audits). * Failure to abide by safeguards would affect accreditation, including the possibility of revocation. |
| 1. Safeguards (requirements) applicable to the Entity Disclosing the Nonpublic Registration Data | The entity disclosing the data:   * Must only supply the data requested by the requestor; * Must return current data in response to a request; * Must monitor the system and take appropriate action, such as revoking or limiting access, to protect against abuse or misuse of the system |
| 1. Safeguards (requirements) applicable to the data subject | The Registered Name Holder (data subject) must have the right:   1. to obtain, on reasonable request, confirmation of the processing of personal data relating to them and the communication in an intelligible form of the data processed    1. Note: When the data subject is shown to have been a secondary victim, this safeguard clearly applies.    2. If the investigator has concluded that the data subject is the perpetrator of a crime, it may not be reasonable to notify the data subject in advance. The decision whether to notify the data subject remains with the data controller.    3. Any system designed for disclosing of data under this use case must include a mechanism for communicating the need for confidentiality.   to obtain, on reasonable request, rectification or erasure, as the case may be, of inaccurate data or data that is being, or has been, processed contrary to the provisions of this Protocol but in the case of erasure, except where that processing is allowed, necessary, or required under applicable law for:  1.       exercising the right of freedom of expression and information;  2.       compliance with a legal obligation(s) for the performance of a task carried out in the public interest;  3.       the exercise of official authority vested in the controller;  4.       reasons of public interest in the area of public health;  5.       archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or  6.       the establishment, exercise or defence of legal claims.     1. not to be subject to a decision significantly affecting them based solely on an automated processing of data unless this is:  * authorized by law providing appropriate safeguards, including at least the right to obtain human intervention; * necessary for entering into, or performance of, a contract between the data subject and a data controller; * authorized by applicable law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or * based on the data subject's explicit consent.   Note that whether decisions referred to herein can be made shall always take into account whether applicable law allows for explicit consent or processing necessary for reasons of substantial public interest.   1. to lodge a complaint with the supervisory authority, or authorities, when they consider that their data protection rights have been violated; 2. to an effective remedy before an independent and impartial tribunal when they consider that their data protection rights have been violated.   Note that the right to object will be limited in instances where applicable law allows for (1) the controller to demonstrate compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject or (2) for the establishment, exercise or defence of legal claims or (3) processing where it is necessary for the performance of a task carried out for reasons of public interest. |
| 1. Safeguards (requirements) applicable to the access/disclosure system | 1. At this stage of an investigation, bulk access[[3]](#footnote-3), wildcard requests, reverse lookups, and boolean search capabilities are not required. 2. Requests must only refer to current registration data (historical registration data will not be made available via this mechanism). 3. Contracted parties are only responsible for disclosing nonpublic registration data for the domain names under their management. 4. Must only return current data (no data about the domain name registration’s history); 5. Must receive a specific request for every individual domain name (no bulk access**[[4]](#footnote-4)**); 6. Must direct requests at the entity that is determined through this policy process to be responsible for the disclosure of the requested data; |
| 1. Accreditation of user group(s) required (Y/N) – if Y, define policy principles | With respect to the accreditation of [user groups] seeking accreditation as a member of this user group must provide:  Evidence of membership in good standing of digital crimes investigations organizations such as   * The Messaging Anti-abuse Working Group ([MAAWG](https://maawg.org/)) * The Anti-phishing Working Group ([APWG](http://apwg.org/)) * The Microsoft Digital Crimes Consortium * National Cyber-Forensics & Training Alliance ([NCFTA](http://ncfta.net/)) * The [U.S. National Cyber Security Alliance](https://staysafeonline.org/) * The [Stop Spam Alliance](http://stopspamalliance.org/) * The London Action Plan ([LAP](http://londonactionplan.com/)) * The U.S. Federal Communications Commission (FCC) Communications Security, Reliability And Interoperability Council ([CSRIC](https://transition.fcc.gov/pshs/advisory/csric/)) * The Anti-spyware Coalition ([ASC](http://antispywarecoalition.org/))   Additional items to be considered in the development of a code of conduct[[5]](#footnote-5):   * All subsequent disclosures to LEA of personal data processed as part of an investigation will be subject to the same levels of lawfulness and auditability as were the initial disclosure to and processing by the digital crimes investigator. * Proof of financial worthiness to justify enhanced access, reverse searching & high volumes (such as bond, letter of credit, insurance, enhanced accreditation fees) |
| 1. Authentication – policy principles |  |
| 1. What information is required to be provided for a request under this lawful basis? |  |
| 1. Expected timing of substantive response | These cases are usually related to transient behavior so instant acknowledgement of the request is critical. |
| 1. Is automation of substantive response possible / desirable? | Automation, if possible, is highly desirable. |
| 1. Expected timing of substantive response | As per (m) above, the decision of the data controller whether to disclose the data should be given the highest priority. |
| 1. How long can the requestor retain the data disclosed and what are the requirements for destruction following the end of the retention period? | Depending on the nature of the investigation, the data may need to be retained for up to 6 months or more in order to support further investigation and/or collaboration with LEA. Deletion following conclusion of investigations should be prompt, although follow-on investigations may occur from time to time. Duration of retention in these cases, and deletion following conclusion of investigations, may be subject to local law related to criminal investigations of this nature. |
| 1. Other? | Regardless of automation, any policy or system designed for disclosing of data under this use case must include a mechanism for communicating the request for confidentiality. |

|  |  |
| --- | --- |
| Use Case: Secondary investigation and identification of other elements within a criminal infrastructure, where domain names are used in the commission of the crime, and where the registrant of domain name(s) has been determined in Part 1 of the use case to be part of ongoing criminal activity –(Part 2 of 2) | |
| 1. User Groups (Requestors) / User characteristics | **Digital crime investigators (corporate or academic). Most investigations of this type start with corporate or academic investigators. LEA relies heavily on these researchers.** |
| 1. Why is non-public registration data necessary? | Non-public registration data is requested in order to identify and confirm additional components of the criminal infrastructure and to identify further investigatory requirements. |
| 1. Data elements that may typically be disclosed[[6]](#footnote-6) | * In this case, it has already been determined that the domain name owner is not a secondary victim but is in fact a perpetrator against the primary victims. The full set of nonpublic data has already been requested in Part 1 of this use case to facilitate further investigation and identification. * Part 2 of this use case relates to pattern-matching portions of the personal data already disclosed in Part 1 against other domain name registrations at the same registrar. * No data elements are disclosed unless the registrar agrees to perform such a search and identifies a match. * If a match is found, the full set of nonpublic data for the matching registrations will be returned. |
| 1. Lawful basis of entity disclosing non-public registration data to the requestor | 6(1)(f) |
| 1. Supporting info to determine lawful basis for the requestor | * Although an investigator may be acting in a fashion which is seemingly in the public interest, GDPR has not yet addressed this type of public interest activity.   + Therefore, like (d) and (e) above, we request that a working party examine the processing required for this use case and provide greater clarity and certainty. * Even in cases where the investigator is doing so at the instruction of LEA, we do not feel that 6(1)(c) is applicable since the investigator is not the data controller.   + Rather, this more clearly falls under the processing contemplated by 6(1)(f).   + Article 10 may also provide justification for such processing. |
| 1. Safeguards (requirements) Applicable to the Requestor | The requestor:   1. Must process data in compliance with data protection laws such as GDPR, including secure transmission; 2. Must provide representations about use of requested data which will be subject to auditing.   Additional items to be considered in the development of a code of conduct[[7]](#footnote-7):  Individuals or entities seeking accreditation as a member of this user group must also:   * Agree to only use the data for the legitimate and lawful purpose described above; * Only issue disclosure requests with respect to the trademark(s) where ownership is evidenced; * Agree to:   + the terms of service, in which the lawful use of data described;   + prevent abuse of data received;   + be subject to de-accreditation if they are found to abuse use of data;   + maintain a register of all requests also including the respective rightsholders name (subject to audits). * Failure to abide by safeguards would affect accreditation, including the possibility of revocation. |
| 1. Safeguards (requirements) applicable to the Entity Disclosing the Nonpublic Registration Data | The entity disclosing the data:   * Must only supply the data requested by the requestor; Note: Absent working party guidance on this use case, it is not yet clear whether data returned as a result of such a request meets the conditions of this safeguard. * Must return current data in response to a request; * Must monitor the system and take appropriate action, such as revoking or limiting access, to protect against abuse or misuse of the system |
| 1. Safeguards (requirements) applicable to the data subject | **The Registered Name Holder** (data subject) must have the same rights as (h) above, with the following caveats:    Regarding the right to obtain, on reasonable request, confirmation of the processing of personal data relating to them and the communication in an intelligible form of the data processed;   * 1. When the data subject is shown to have been a secondary victim, this safeguard clearly applies.   2. In this use case, it has already been determined that they are not such a victim but rather are engaged in criminal activity.   3. Since the investigator has concluded that the data subject is the perpetrator of a crime, it is not reasonable to notify them in advance. The decision not to notify the data subject remains with the data controller. |
| 1. Safeguards (requirements) applicable to the access/disclosure system | 1. At this stage of an investigation, bulk access[[8]](#footnote-8), wildcard requests, reverse lookups, and boolean search capabilities may be required, but such searches must be conducted by the data controller and are only at the discretion of the data controller. 2. Requests must only refer to current registration data (historical registration data will not be made available via this mechanism). 3. Contracted parties are only responsible for disclosing nonpublic registration data for the domain names under their management. 4. Must only return current data (no data about the domain name registration’s history); 5. Must receive a specific request for every individual domain name (no bulk access**[[9]](#footnote-9)**), except atthe discretion of the data controller; 6. Must direct requests at the entity that is determined through this policy process to be responsible for the disclosure of the requested data |
| 1. Accreditation of user group(s) required (Y/N) – if Y, define policy principles | With respect to the accreditation of [user groups] seeking accreditation as a member of this user group must provide:  Evidence of membership in good standing of digital crimes investigations organizations such as   * The Messaging Anti-abuse Working Group ([MAAWG](https://maawg.org/)) * The Anti-phishing Working Group ([APWG](http://apwg.org/)) * The Microsoft Digital Crimes Consortium * National Cyber-Forensics & Training Alliance ([NCFTA](http://ncfta.net/)) * The [U.S. National Cyber Security Alliance](https://staysafeonline.org/) * The [Stop Spam Alliance](http://stopspamalliance.org/) * The London Action Plan ([LAP](http://londonactionplan.com/)) * The U.S. Federal Communications Commission (FCC) Communications Security, Reliability And Interoperability Council ([CSRIC](https://transition.fcc.gov/pshs/advisory/csric/)) * The Anti-spyware Coalition ([ASC](http://antispywarecoalition.org/))   Additional items to be considered in the development of a code of conduct[[10]](#footnote-10):   * All subsequent disclosures to LEA of personal data processed as part of an investigation will be subject to the same levels of lawfulness and auditability as were the initial disclosure to and processing by the digital crime investigator. * Proof of financial worthiness to justify enhanced access, reverse searching & high volumes (such as bond, letter of credit, insurance, enhanced accreditation fees) |
| 1. Authentication – policy principles |  |
| 1. What information is required to be provided for a request under this lawful basis? | Whatever applies to (l) above also applies here.  Additionally, the data controller may request additional proof that the data subject is not a secondary victim. |
| 1. Expected timing of substantive response | These cases are usually related to transient behavior so instant acknowledgement of the request is critical. |
| 1. Is automation of substantive response possible / desirable? | Automation is not available |
| 1. Expected timing of substantive response | * As per (m) above, the decision of the data controller whether to disclose the data should be given the highest priority. * Response timing may be subject to processing limitations of the data controller |
| 1. How long can the requestor retain the data disclosed and what are the requirements for destruction following the end of the retention period? | Similar to (p) above, retention period is dependent on the nature of the investigation. The data may need to be retained for up to 6 months or more in order to support further investigation and/or collaboration with LEA. Deletion following conclusion of investigations should be prompt, although follow-on investigations may occur from time to time. Duration of retention in these cases, and deletion following conclusion of investigations, may be subject to local law related to criminal investigations of this nature. |
| 1. Other? | Regardless of automation, any policy or system designed for disclosing of data under this use case must include a mechanism for communicating the request for confidentiality and a mechanism for providing additional proofs to the data controller. |

1. For each request, the requestor will need to confirm which data elements are necessary. [↑](#footnote-ref-1)
2. The code of conduct referenced within this table is distinct from the code of conduct referenced in [Section 3.7.1 of the Registrar Accreditation Agreement](http://www.icann.org/2013raa#3.7.1). [↑](#footnote-ref-2)
3. As defined in section 3.3.6 of the Registrar Accreditation Agreement [↑](#footnote-ref-3)
4. As defined in section 3.3.6 of the Registrar Accreditation Agreement. [↑](#footnote-ref-4)
5. The code of conduct referenced within this table is distinct from the code of conduct referenced in [Section 3.7.1 of the Registrar Accreditation Agreement](http://www.icann.org/2013raa#3.7.1). [↑](#footnote-ref-5)
6. For each request, the requestor will need to confirm which data elements are necessary. [↑](#footnote-ref-6)
7. The code of conduct referenced within this table is distinct from the code of conduct referenced in [Section 3.7.1 of the Registrar Accreditation Agreement](http://www.icann.org/2013raa#3.7.1). [↑](#footnote-ref-7)
8. As defined in section 3.3.6 of the Registrar Accreditation Agreement [↑](#footnote-ref-8)
9. As defined in section 3.3.6 of the Registrar Accreditation Agreement. [↑](#footnote-ref-9)
10. The code of conduct referenced within this table is distinct from the code of conduct referenced in [Section 3.7.1 of the Registrar Accreditation Agreement](http://www.icann.org/2013raa#3.7.1). [↑](#footnote-ref-10)