

Network Working Group
Internet-Draft
Intended status: Informational
Expires: 13 October 2025

D. James
Marashlian & Donahue, PLLC
T. McCarthy-Howe
Strolid
11 April 2025

Privacy Primer for vCon Developers
draft-james-privacy-primer-vcon-01

Abstract

This document serves as a primer for technical professionals involved in managing personal data, including biometric information from audio and video recordings, and other sensitive information in messaging or personal communications. It outlines key concepts in data privacy and communications privacy, addressing the ethical and legal considerations surrounding the collection, processing, and disclosure of consumer data. The document covers fundamental privacy principles, defines important roles in data processing, and explains consumer rights regarding their personal information. It also discusses the scope of protected personal information, including sensitive data categories, and explores techniques like data aggregation and anonymization. While referencing existing IETF work on privacy in Internet communications, this draft extends beyond to address consumer data privacy in relation to organizations handling such data. The goal is to provide a comprehensive overview of privacy considerations, aligning with fair information practices and current regulatory frameworks, to guide professionals in implementing privacy-respecting data management practices.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at <https://howethomas.github.io/privacy-primer-vcon/draft-james-privacy-primer-vcon.html>. Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-james-privacy-primer-vcon/>.

Source for this draft and an issue tracker can be found at <https://github.com/howethomas/privacy-primer-vcon>.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 13 October 2025.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

- 1. Introduction
 - 1.1. Purpose of this Document
 - 1.2. Intended Audience
 - 1.3. Goals of this Document
- 2. Conventions and Definitions
- 3. Goal
 - 3.1. Privacy and vCon In General
 - 3.2. Data privacy
 - 3.2.1. Key Roles in Data Processing
 - 3.2.2. What Rights in Their Data do Consumers Have?
 - 3.2.3. What Data Is Protected?
 - 3.2.4. Sensitive Data
 - 3.2.5. What Data Isn't Protected?
 - 3.2.6. Aggregation/Anonymization
 - 3.3. Communications Privacy
 - 3.3.1. Key Privacy Principles
- 4. Security Considerations
- 5. IANA Considerations
 - 5.1. Informative References
- 6. Normative References
- Acknowledgments
- Authors' Addresses

1. Introduction

The democratization of technology has led to a surge of new entrants in the growing market of personal data management. These entrants, driven by various motives ranging from commerce and regulation to fraud prevention and charitable causes, are increasingly engaging with conversational data across network boundaries. The vCon (Virtual Conversation) represents a significant step forward in this landscape, enabling the ethical sharing of conversational data and fostering a rich ecosystem of services based on a novel concept: genuinely listening to what customers say.

However, many of these new entrants may not inherently understand the ethical and legal complexities surrounding crucial topics such as data minimization, redaction, the right to know, and the right to erasure. The design decisions behind the vCon framework directly address these concerns, incorporating features such as encryption capabilities, external data signing for change detection, and the creation of redacted versions that maintain a trail to the original data.

1.1. Purpose of this Document

This document serves as a primer for individuals and organizations grappling with the challenges of responsible personal data management in the digital age. It aims to provide a foundational understanding of key topics, explaining their importance and how they are addressed (or not) within the vCon framework. While the vCon is not a panacea, it offers a structure that enables well-intentioned actors to operate

ethically and responsibly. Much like the distinction between HTTP and HTTPS, where HTTPS is trusted by default and HTTP is not, the vCon framework provides a basis for trust, with legal systems managing those who operate outside its principles.

1.2. Intended Audience

This primer is designed to cater to three primary constituencies often present in IETF discussions:

- * **Technologists and Engineers:** Often immersed in technical details, these professionals may benefit from understanding the broader ethical and legal considerations that should inform their designs. This document aims to bridge the gap between technical implementation and important "non-technical" issues they need to consider.
- * **Regulators, Lawyers, and Government Representatives:** Responsible for tech policy, these individuals often approach discussions with the perspectives of their constituencies but are generally open to education. This document seeks to provide them with a clearer understanding of how their legal concerns are addressed within the vCon framework and what aspects fall outside its scope.
- * **Non-Governmental Organizations (NGOs):** Particularly those focused on privacy, security, and human rights, these organizations represent the intersection of policy and technology. Often skeptical of commercial and government interests, this audience will find information on how the vCon supports personal data privacy, transparency, and control.

1.3. Goals of this Document

The primary objectives of this primer are:

- * To educate an expanding audience on the fundamental concepts of responsible customer data management.
- * To foster a common understanding of the challenges involved in personal data handling.
- * To provide an informed perspective on what is currently addressed by the vCon framework and what remains outside its scope.
- * To encourage thoughtful consideration of ethical and legal issues in the design and implementation of systems handling personal data.

By achieving these goals, we aim to contribute to a more informed and responsible approach to personal data management across various sectors and disciplines.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Goal

To act as a primer to technical professionals involved with managing personal data, including biometric information contained in audio and video recordings, or other sources of sensitive information, in messaging or other personal communications. Issues, ethics,

legalities and relevant IETF work should be referenced as appropriate.

IETF standards already address privacy in Internet communications, including the principle of data minimization [RFC 7258]. However, those standards generally do not address consumer data privacy vis-à-vis organizations that collect, process, and disclose consumer data.

3.1. Privacy and vCon In General

Privacy in general can be understood as "the right to be let alone" [Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review, 4(5), 193-220]. It may be helpful to think of it in four aspects:

1. personal information (or data) privacy,
2. bodily privacy,
3. territorial privacy, and
4. communications privacy.

In the context of vCon, we will concentrate on **data privacy** and **communications privacy**.

3.2. Data privacy

Data privacy, also known as information privacy or data protection, refers to the practice of safeguarding individuals' personal information from unauthorized access, use, disclosure, alteration, or destruction. It involves ensuring that individuals have control over their own personal data and that organizations that collect, store, and process personal data do so in a manner that respects individuals' privacy rights.

Data privacy laws and regulations vary by jurisdiction, but many countries and regions have enacted legislation to protect individuals' personal data. Examples of data privacy laws include the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and the Personal Data Protection Act (PDPA) in Singapore. The U.S. data privacy legal landscape is a particularly complex patchwork of federal and state laws. It includes comprehensive state-level consumer privacy acts, industry-specific federal laws, and intricate pre-emption relationships between them, creating a fragmented and multifaceted regulatory environment.

This document outlines common privacy rights and obligations in alignment with fair information practices (FIP), which are widely recognized principles but may or may not be legally required, depending on the jurisdiction. The framework presented here offers a general understanding of data privacy principles but does not guarantee legal compliance in any specific region. Readers are encouraged to seek legal advice for their particular situations.

3.2.1. Key Roles in Data Processing

The following terms are used by the GDPR and in the privacy industry in general to define the three key roles in data processing:

1. **Data Subject**: The individual whose personal information is being processed (also referred to as "consumer" in this RFC and many personal data privacy laws).

2. ***Data Controller***: An organization or individual with decision-making authority over data processing who determines the purposes and methods of data processing, bears primary responsibility under privacy laws and is the main target of most privacy and data protection regulations.
3. ***Data Processor***: Often a third-party service provider who processes data on behalf of the data controller. Under HIPAA, data processors are referred to as "business associates." Data processors may be hired for specialized tasks or to improve efficiency; can subcontract to other processors, creating a chain of responsibility; must operate within the scope defined by the data controller; and are expected to maintain trust and adhere to the controller's guidelines.

The relationship between these entities forms a hierarchy of responsibility and trust. The data controller sets the parameters for data use, while processors at various levels must operate within these boundaries. This structure ensures accountability and helps maintain data privacy throughout the information processing chain.

3.2.2. What Rights in Their Data do Consumers Have?

Regarding individual rights in data privacy, organizations should focus on six key areas:

1. ***Notice of Data Processing***: Organizations must clearly communicate their privacy policies and practices. This includes explaining what personal data is collected and for which purposes, how it is used, stored, and shared, and how consumers can exercise their data privacy rights. This ensures transparency, holds data controllers accountable, and empowers individuals to make informed choices about their personal information.
2. ***Consent***: Organizations need to obtain data subjects' informed and freely given consent for collecting, using, storing, and sharing personal data. Different levels of consent may apply to different kinds of data or in different jurisdictions:
 - * Consent can be affirmative ("opt-in" consent) or presumed unless stated otherwise ("opt-out" consent). Opt-in consent is usually required for sensitive data and children's data (under 13 or 16 years old).
 - * Consent can be written, oral, or implied.
 - * In some jurisdictions, such as California, consent must be sought at or before the point of data collection.
3. ***Access***: Organizations should offer mechanisms for consumers to access and correct their personal data. This empowers people to ensure their data is accurate and up-to-date.
4. ***Data Choices***: In addition to rights to access and correct, data subjects often have the following data privacy rights:
 - * right to have their information deleted (also referred to as the "right to be forgotten");
 - * right to port their data to a different data controller;
 - * right opt out of certain data practices, such as sale of their data, profiling, targeted/cross contextual behavioral advertising, automated decision-making.

5. ***Non-Discrimination*:** Organizations must not discriminate against consumers who choose to exercise their data privacy rights.
6. ***Breach Notification*:** The large amounts of data held by organizations attracts cybercriminals, increasing the risk of data breaches. To mitigate the consequences of data breaches and incentivize advanced data security practices, most jurisdictions require prompt notification of affected individuals when breaches occur (within 30 days of discovery being the industry practice in the U.S.). This holds organizations accountable for data security and allows individuals to take protective actions.

By addressing these areas, organizations can respect individual privacy rights and build trust with their customers or users. This approach aligns with many modern data protection regulations and best practices in privacy management.

3.2.3. What Data Is Protected?

Data privacy laws protect personal information, though its scope can vary across different laws. In general, the term "personal information" (also known as "personally identifiable information" or "PII") includes information that makes it possible to identify an individual or information about an "identified" or "identifiable" individual. California extends the scope of PII to include information about a consumer and the consumer's household, as well as employment data. Examples of PII include:

- * Basic identifiers: Name, addresses (postal and email), government-issued identification numbers
- * Digital identifiers: IP address (in some jurisdictions like California).
- * Financial Data: financial account number or credit or debit card number, often in combination with any required security code or password that would permit access to a data subject's financial account.
- * Protected characteristics: Race, religion, disability, sexual orientation, national origin, etc.
- * Consumer behavior: Purchase history, product interests, consumption patterns.
- * Biometric data, including voiceprints, faceprints, fingerprints.
- * Online activity: Browsing and search history, website and app interaction.
- * Geolocation information
- * Sensory information: Audio, visual, thermal, and olfactory data.
- * Professional and educational information.

3.2.4. Sensitive Data

An important subset of PII to consider in designing data privacy practices is so-called "sensitive data" which is subject to a higher standard of protection and requires additional privacy and security limitations to safeguard its collection, use and disclosure. For example, it may require an opt-in consent for data collection and processing. In various jurisdictions sensitive information may include the following:

- * Government-issued identifiers.
- * Physical or mental health information.
- * Genetic data.
- * Financial data.
- * Biometric information.
- * Precise geolocation data (information on a customer's location within a 1,850-foot radius around the consumer).
- * Certain communications data an individual's private communications, such as voicemails, emails, texts, direct messages or mail, or information identifying the parties to such communications, information contained in telephone bills, voice communications, and any information that pertains to the transmission of voice communications, including numbers called, numbers from which calls were placed, the time calls were made, call duration and location information of the parties to the call, unless the covered entity is an intended recipient of the communication. Communications with businesses may be awarded less protection.
- * Log-in credentials a customer's account log-in, password, or credentials allowing access to an account.
- * Citizenship and immigration status.
- * Sexual behavior.
- * Less commonly - *calendars, address book information, phone or text logs, photos, audio recordings, or videos intended for private use* typically stored on smartphones and tablets that reveal personal information about an individual's daily habits and social interactions.
- * Less commonly - *transferred video viewing habit information* - information revealing the extent or content of any individual's access, viewing or other use of any video programming, including by a provider of broadcast television service, cable service, satellite service or streaming media service, but only concerning the transfer of such information to a third party and excluding any such data used solely for transfers for independent video measurement.
- * *Online activity -* information revealing an individual's online activities over time and across websites or online services that do not share common branding or over time on any website or online service operated by a covered high-impact social media company.
- * Information about minors (17 years of age or younger).

3.2.5. What Data Isn't Protected?

The distinction between personal and nonpersonal information hinges on identifiability. This boundary can be ambiguous, with varying interpretations across jurisdictions. For instance, IP addresses are considered personal information by the EU and FTC, but not by U.S. federal agencies under the Privacy Act.

When identifying elements are removed from data, it becomes nonpersonal information, generally falling outside the scope of privacy and data protection laws. This process, known as *deidentification or anonymization*, is often used for research,

statistics, or aggregated data analysis. Several U.S. state comprehensive privacy laws exclude deidentified and aggregate data from the scope of personal information.

Pseudonymized data, where individuals are represented by unique codes, is temporarily nonpersonal but can be reversed to reidentify individuals. This reversibility can be crucial in scenarios like medical trials. In many jurisdictions pseudonymous data falls within the scope of personal data when used in conjunction with additional information that reasonably links the data to an identified or identifiable individual.

Many jurisdictions remove **publicly available information** from the scope of protected PI.

3.2.6. Aggregation/Anonymization

Data aggregation and anonymization are important techniques used in the context of data privacy to protect individuals' personal information while still allowing organizations to derive valuable insights. However, these methods are not without risks and limitations.

Data aggregation involves combining data from multiple sources or individuals into summary form. While this can obscure individual identities, there are still privacy concerns:

1. **Re-identification risk**: With enough granular data points, it may be possible to single out individuals even from aggregated datasets. Applying multiple specific filters to aggregate data could potentially identify a unique individual.
2. **Inference attacks**: Aggregated data can reveal patterns that allow inferences about individuals or small groups, even if direct identifiers are removed.
3. **Unintended data exposure**: As aggregated data is often shared between organizations, there's increased risk of unauthorized access or misuse.

Anonymization aims to remove or encrypt personal identifiers from datasets. However, true anonymization is challenging:

1. **De-identification limitations**: Simply removing obvious identifiers like names and addresses is often not sufficient to prevent re-identification. Indirect identifiers can still allow individuals to be singled out.
2. **Data utility trade-offs**: More thorough anonymization techniques tend to reduce the usefulness of the data for analysis.
3. **Evolving re-identification techniques**: As technology advances, previously anonymized data may become vulnerable to new re-identification methods.

To mitigate these risks, organizations should consider:

1. Implementing robust anonymization techniques beyond basic de-identification.
2. Carefully assessing the granularity and specificity of aggregated data released.
3. Combining anonymization with other privacy-enhancing technologies like differential privacy.

4. Conducting regular privacy impact assessments to evaluate potential risks.
5. Adhering to relevant privacy regulations and best practices for data handling.

While data aggregation and anonymization can enhance privacy protection, they should not be viewed as foolproof solutions. Organizations must remain vigilant and adopt a comprehensive approach to data privacy that considers the evolving nature of re-identification risks and the potential for unintended consequences when working with large datasets.

3.3. Communications Privacy

Communications privacy is a critical concern in our increasingly interconnected world, where various forms of communication including audio, video, text messages, and emails have become integral to both personal and professional interactions. Under the applicable laws, communications are protected when in transit and when stored.

Understanding the multifaceted legal and ethical frameworks around communications privacy is essential for anyone involved in capturing, storing, analyzing, or managing communications data. Communications privacy laws across various jurisdictions often share common elements, designed to protect individuals' privacy rights while balancing the needs of law enforcement and legitimate business interests. Here are some key provisions typically found in laws governing the recording, interception, eavesdropping, and storage of communications:

1. ***Notice:** Many laws require that parties be notified if their communications are being recorded or monitored, often through audible beeps, verbal announcements, or visible signage. The unauthorized surveillance or interception of an individual's private communications or activities is generally prohibited by law.
2. ***Consent:** Many laws stipulate that at least one party must consent to the recording or interception of a communication. Some jurisdictions require all parties to consent, known as "two-party" or "all-party" consent. The type of consent required (explicit or implied) may vary, but it has to be obtained prior to the recording.
3. ***Distinction Between Public and Private Communications:** Laws often differentiate between communications where there is a reasonable expectation of privacy (e.g., private phone calls) and those in public spaces where such expectation may not exist.
4. ***Purpose Limitations:** Regulations frequently specify permissible purposes for recording or intercepting communications, such as for security, quality assurance, or with court authorization for law enforcement activities.
5. ***Storage and Retention Limitations:** Rules governing how long recorded communications can be stored, how they must be protected, and when they should be destroyed are common features of privacy laws.
6. ***Exceptions for Law Enforcement:** Most laws include provisions allowing for authorized interception of communications by law enforcement agencies, typically requiring judicial oversight through warrants or court orders.

7. ***Technology-Specific Provisions***: As technology evolves, laws may include specific provisions for different communication media, such as landlines, mobile phones, emails, instant messaging, video calls, and Internet browsing activities.
8. ***Security Measures***: Requirements for securing stored communications against unauthorized access, including encryption standards and access controls, are increasingly common.

Understanding these common provisions is crucial for compliance with communications privacy laws, regardless of the specific jurisdiction. However, it is important to note that the exact implementation and interpretation of these provisions can vary significantly between different legal frameworks.

3.3.1. Key Privacy Principles

Data privacy and communications privacy are guided by similar principles, emphasizing consent, transparency, and data minimization while balancing privacy rights with societal interests. These areas aim to safeguard individuals' control over their personal information, whether stored or transmitted. Key principles include:

1. ***Consent***: Must be freely given, specific, informed, unambiguous, revocable, and documented. Consent may not be valid in situations with power imbalances or required when processing is necessary to satisfy legal obligations or implement contracts. So-called "dark patterns," which are practices of seeking consent that effectively obscure, subvert, or impair the consumer's autonomy, decision-making or choice (for example, confusing user interfaces or hidden disclosures) are not allowed in most jurisdictions.
2. ***Notice/Transparency***: Organizations must clearly disclose their data handling practices. Privacy notices should be concise, transparent, and easily understood. Changes to privacy practices must be promptly communicated.
3. ***Purpose Limitation***: Personal data should be collected for specific, explicit, and legitimate purposes, and it should not be used for purposes that are incompatible with those for which it was originally collected.
4. ***Data Minimization/Collection Limitation***: Organizations should collect only the minimum amount of personal data necessary to achieve the stated purpose. Excessive or irrelevant data should not be collected.
5. ***Storage Limitation***: Personal data should be retained only for as long as necessary to fulfill the purposes for which it was collected. Organizations should establish retention policies and securely dispose of data that is no longer needed.
6. ***Security***: Appropriate technical and organizational measures must be implemented to protect personal data from unauthorized access and other risks. This may include encryption, access controls, and regular security assessments.
7. ***Individual Rights***: Individuals have certain rights regarding their personal data, including the right to access their data, the right to request corrections or deletions ("the right to be forgotten"), the right to object to certain uses of their data, and the right to data portability (the ability to transfer their data from one organization to another).
8. ***Accuracy***: Personal data should be accurate, complete, and up-

to-date.

9. *Accountability*: Organizations are responsible for complying with data privacy laws and demonstrating compliance. This may involve conducting privacy impact assessments, appointing a data protection officer, and maintaining records of data processing activities.
10. *Recordkeeping*: Maintain accurate logs of consumers' profiles, data decisions, and data usage, including sales and marketing campaigns and instances of data disclosure to third parties.

While data privacy and communications privacy share many principles, there are some distinctions in their regulation. Communications privacy laws often focus more on real-time interception and communication confidentiality, while data privacy laws address a broader range of data handling practices.

As the digital landscape evolves, privacy laws must continually adapt to address emerging technologies and practices, ensuring the protection of personal information in our interconnected world.

4. Security Considerations

vCons contain sensitive conversational data, which raises several security concerns, particularly regarding data integrity and personal privacy. The following points outline the key security considerations for vCons:

1. Data Integrity and Immutability

- * vCons need to be protected against unauthorized modifications to ensure the authenticity of the conversational data.
- * Before a vCon leaves its original security domain, it should be digitally signed to prevent alteration, as specified in Section 5.2 (Signed Form of vCon Object).

2. Privacy Protection

- * vCons often contain personally identifiable information (PII) and sensitive data that must be safeguarded.
- * Different levels of redaction may be necessary, as outlined in Section 4.1.6 (redacted): a) PII masking: Removing PII from text, audio, video, and transcripts b) De-identification: Removing segments or whole recordings to prevent voice printing or facial recognition

3. Encrypted Storage and Transmission

- * Unredacted versions of vCons must be encrypted to protect sensitive information, as described in Section 5.3 (Encrypted Form of vCon Object).
- * vCons transmitted over non-secure channels (e.g., email) must always be in encrypted form.

4. Access Control

- * Externally referenced files should be transported only over HTTPS, as specified in Section 2.4 (Externally Referenced Files).
- * Access to unredacted vCons and their referenced files should be restricted to authorized personnel only.

5. Version Management

- * Multiple versions of a vCon may exist (e.g., redacted versions, versions with added analysis).
- * Each version must maintain its own integrity while providing a secure reference to its predecessor, as described in Sections 4.1.6 (redacted) and 4.1.7 (appended).

6. Cross-Domain Security

- * vCons may be created and modified across different security domains, as discussed in Section 4 (Unsigned Form of vCon Object).
- * Each domain should sign the vCon before transferring it to maintain the chain of trust, using the method in Section 5.2 (Signed Form of vCon Object).

7. Redaction Processes

- * While methods exist for redacting text, audio, and video, the specific techniques are beyond the scope of the vCon standard, as noted in Section 4.1.6 (redacted).
- * Implementers must ensure that redaction methods effectively remove sensitive information without compromising the vCon's integrity.

8. Balancing Utility and Privacy

- * There's an inherent tension between maintaining the usefulness of vCons and protecting privacy, as implied throughout Section 4 (Unsigned Form of vCon Object).
- * Careful consideration is needed when deciding what information to redact or encrypt.

9. Encryption of Referenced Content

- * Externally referenced files that are part of a vCon should be encrypted if they contain sensitive information, as suggested in Section 2.4 (Externally Referenced Files).

10. Audit Trail

- * vCons should maintain a secure audit trail of modifications, especially for redactions and additions, to ensure accountability. This is supported by the structure described in Sections 4.1.6 (redacted) and 4.1.7 (appended).

By addressing these security concerns and following the guidelines in the vCon standard, implementers can help ensure that vCons protect the privacy of individuals involved in conversations while maintaining the integrity and utility of the conversational data.

5. IANA Considerations

This document has no IANA actions.

5.1. Informative References

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, July 2013, <https://www.rfc->

editor.org/info/rfc6973 (<https://www.rfc-editor.org/info/rfc6973>).

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, May 2014, <https://www.rfc-editor.org/info/rfc7258> (<https://www.rfc-editor.org/info/rfc7258>).

[RFC8280] ten Oever, N. and C. Cath, "Research into Human Rights Protocol Considerations", RFC 8280, October 2017, <https://www.rfc-editor.org/info/rfc8280> (<https://www.rfc-editor.org/info/rfc8280>).

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003, <https://www.rfc-editor.org/info/rfc3552> (<https://www.rfc-editor.org/info/rfc3552>).

[RFC7624] Barnes, R., Schneier, B., Jennings, C., Hardie, T., Trammell, B., Huitema, C., and D. Borkmann, "Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement", RFC 7624, August 2015, <https://www.rfc-editor.org/info/rfc7624> (<https://www.rfc-editor.org/info/rfc7624>).

[RFC6462] Cooper, A., "Report from the Internet Privacy Workshop", RFC 6462, January 2012, <https://www.rfc-editor.org/info/rfc6462> (<https://www.rfc-editor.org/info/rfc6462>).

[RFC7844] Huitema, C., Mrugalski, T., and S. Krishnan, "Anonymity Profiles for DHCP Clients", RFC 7844, May 2016, <https://www.rfc-editor.org/info/rfc7844> (<https://www.rfc-editor.org/info/rfc7844>).

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, August 2018, <https://www.rfc-editor.org/info/rfc8446> (<https://www.rfc-editor.org/info/rfc8446>).

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, May 2016, <https://www.rfc-editor.org/info/rfc7858> (<https://www.rfc-editor.org/info/rfc7858>).

[RFC6235] Boschi, E. and B. Trammell, "IP Flow Anonymization Support", RFC 6235, May 2011, <https://www.rfc-editor.org/info/rfc6235> (<https://www.rfc-editor.org/info/rfc6235>).

[RFC8165] Hardie, T., "Design Considerations for Metadata Insertion", RFC 8165, May 2017, <https://www.rfc-editor.org/info/rfc8165> (<https://www.rfc-editor.org/info/rfc8165>).

[RFC7011] Claise, B., Ed., Trammell, B., Ed., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, September 2013, <https://www.rfc-editor.org/info/rfc7011> (<https://www.rfc-editor.org/info/rfc7011>).

6. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/rfc/rfc2119>>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/rfc/rfc8174>>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Diana James
Marashlian & Donahue, PLLC
Email: daj@commlawgroup.com

Thomas McCarthy-Howe
Strolid
Email: thomas.howe@strolid.com