



DEPARTMENT OF JUSTICE | OFFICE OF THE INSPECTOR GENERAL

MANAGEMENT ADVISORY MEMORANDUM

25-085

SEPTEMBER 2025

Notification of Concerns Regarding the Need
for Grant Recipients to Safeguard Victim
Information When Using Various
Technologies

AUDIT DIVISION



September 16, 2025

Management Advisory Memorandum

To: Maureen A. Henneberg
Deputy Assistant Attorney General for Operations and Management
Office of Justice Programs

Ginger Baran Lyons
Deputy Director for Grants Development and Management
Office on Violence Against Women

From: William M. Blier
Acting Inspector General

Subject: Notification of Concerns Regarding the Need for Grant Recipients to Safeguard Victim Information When Using Various Technologies

The purpose of this memorandum is to advise you of concerns identified during Office of the Inspector General (OIG) grant audits related to the need for grant recipients to safeguard victim information when using or employing existing or emerging technologies.

The OIG's prior grant audit work has repeatedly identified privacy and confidentiality concerns related to the use of ridesharing applications (apps). Our concerns in this area prompted us to consider other potential areas of risk that may affect victims, many of whom are served by Department of Justice grants made by the Office of Justice Programs (OJP) and the Office on Violence Against Women (OVW). Additional risks include, but are not limited to, the use of social media in a manner that could disclose identity or location information, the use or misuse of Global Positioning Services, including location services or physical tracking tags, and spyware tools.¹ These apps, in addition to some payment and ridesharing apps, present the risk that a victim's location can be identified by an abuser. If appropriate measures are not taken to use these technologies safely, a victim's abuser can easily exploit these technologies to cause harm, including to persons provided services and assistance through Department of Justice (DOJ)-funded grants.

Summary of Previously Reported Information

The OIG has previously highlighted victim-related confidentiality and privacy issues with grant recipients' use of ridesharing apps in several of our grant audits. A February 2024 report revealed that an OJP Office for Victims of Crime (OVC) funding recipient used ridesharing services to transport victims but lacked formal

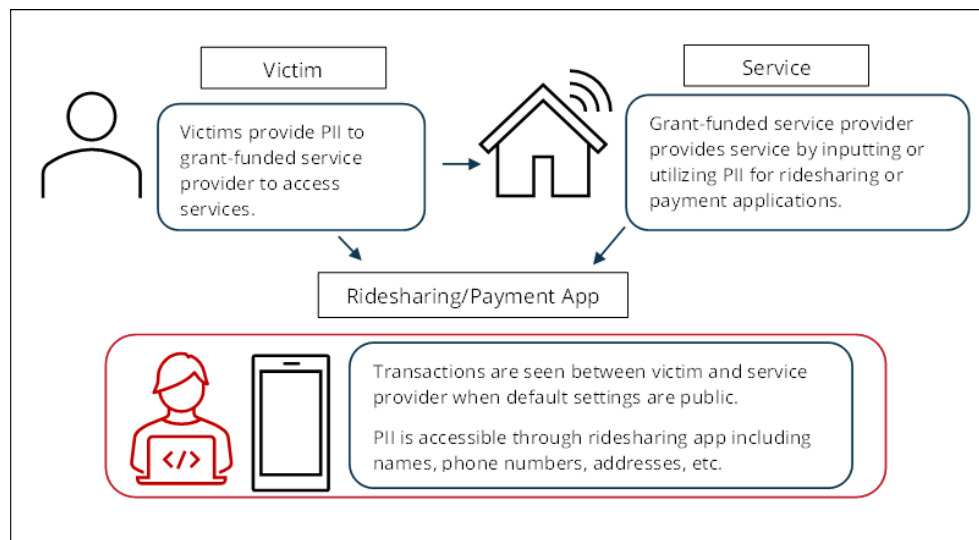
¹ National Institutes of Health's National Library of Medicine, "[Safeguarding patients from technology-facilitated abuse in clinical settings: A narrative review](https://pubmed.ncbi.nlm.nih.gov/articles/PMC9931347/)," PMID 9931347, January 4, 2023, <https://pubmed.ncbi.nlm.nih.gov/articles/PMC9931347/> (accessed April 2025).

policies and procedures to safeguard victim personally identifiable information (PII), such as names and phone numbers.² Additionally, a September 2023 report identified an OVC subrecipient's lack of policies and procedures to prevent the submission of sensitive and confidential information to taxi and ridesharing services to transport victims between the shelter and service providers.³ Similarly, a May 2023 report found another OVC funding recipient lacked procedures to safeguard its ridesharing account from unauthorized use.⁴ Relatedly, in July 2024, the victim-related risks associated with the use of payment apps were highlighted by an investigative journalist who reported being able to identify several residents at a domestic violence "safe house" through public payment transactions to the service provider.⁵ These situations highlight serious concerns about how abusers can exploit information collected by certain apps to access information about victims, including their location.

As shown in Figure 1 below, depending on privacy settings, transactions in some apps can be seen by anyone with access to the account, such as an abusive partner, or even the public. This may include full names, phone numbers, and home or safe house addresses.

Figure 1

Potential Victim PII Accessibility When Using Ridesharing/Payment Applications



Source: OIG

² U.S. Department of Justice (DOJ) Office of the Inspector General (OIG), *Audit of the Office of Justice Programs Victim Assistance Funds Subawarded by the Maryland Governor's Office of Crime Prevention, Youth, and Victim Services to the University of Maryland Prince George's Hospital Center in Largo, Maryland*, Audit Report 24-030 (February 2024), oig.justice.gov/reports/audit-office-justice-programs-victim-assistance-funds-subawarded-maryland-governors-0.

³ DOJ OIG, *Audit of the Office of Justice Programs Victim Assistance Funds Subawarded by the Minnesota Department of Public Safety Office of Justice Programs to Women of Nations, Incorporated, Saint Paul, Minnesota*, Audit Report 23-111 (September 2023), oig.justice.gov/reports/audit-office-justice-programs-victim-assistance-funds-subawarded-minnesota-department.

⁴ DOJ OIG, *Audit of the Office of Justice Programs Victim Assistance Funds Subawarded by the Colorado Division of Criminal Justice to the Rose Adom Center, Denver, Colorado*, Audit Report 23-072 (May 2023), oig.justice.gov/reports/audit-office-justice-programs-victim-assistance-funds-subawarded-colorado-division-0.

⁵ Kelsey Turner and Wilson Criscione, "Idaho local and state agencies directed federal funding to safe house despite complaints and contractual violations," *InvestigateWest*, July 16, 2024, www.investigatwest.org/investigatwest-reports/idaho-local-and-state-agencies-directed-federal-funding-to-safe-house-despite-complaints-and-contractual-violations-17706780 (accessed November 2024).

Privacy and Confidentiality Policies

In today's data-rich environment, numerous state and federal laws protect data privacy and the confidentiality of PII in professional relationships. The U.S. Congress has codified victim confidentiality in the Violence Against Women Act (34 U.S.C. § 12291), the Family Violence Prevention and Services Act (42 U.S.C. § 10401), and the Victims of Crime Act of 1984 (34 U.S.C. § 20101 et seq.). These laws prohibit sharing PII about victims without informed, written, time-limited consent, and they generally prohibit disclosure of individual information without written consent. Additionally, some OJP and OVW victim-related awards include measures to address victim confidentiality and privacy, such as requiring written policies to maintain confidentiality and guidance on reporting breaches.

Moreover, many apps, including ridesharing and payment apps, include privacy measures such as limiting PII access and data encryption, but they still pose privacy risks. According to publicly available privacy policies, users are cautioned that some default privacy settings are public, making transactions and PII accessible to anyone on the internet unless manually set to private. Data tracking and sharing with third parties are also often enabled by default without users' explicit consent.

Conclusion

We discussed our concerns with OJP and OVW officials about the need to take action to ensure that victim-related PII is secured by recipients of its funding, particularly as technology evolves at a rapidly increasing pace. These officials outlined ongoing work, such as the creation of a working group focused on victim confidentiality concerns. We also were told that OVW reached out to a technical assistance provider and determined that the provider had previously worked with a ridesharing company to develop a victim-centered safety and privacy considerations resource guide.⁶ The resource guide and safety tipsheet suggest certain actions that protect against the dissemination of victim PII, such as utilizing the Safety Check feature on devices or using gift cards or prepaid cards to pay for ride services. However, we note that neither the resource guide nor the safety tipsheet have been distributed directly to the DOJ grant recipient community that provide services to victims.

The OIG acknowledges DOJ granting agencies' existing commitment to victim privacy, and we believe OJP and OVW can further collaborate to identify ways in which the DOJ can raise awareness among its grant funding recipients of the need to mitigate risks to victims associated with emerging technology. The risks that may compromise victim safety include, but are not limited to, ridesharing, payment, and social media apps; victims' mobile phone location sharing settings; and shared devices or accounts. We are highlighting this issue with the aim that DOJ granting agencies help enhance victim safety and PII protection by working with DOJ grant recipients on safer uses of technology that pose risks to victim safety and PII.

Recommendation

We recommend that OJP and OVW:

1. Coordinate and take actions to raise awareness among grant recipients on mitigating risks to victim safety that can occur through the use of technologies that store PII and location information.

We previously furnished you with copies of a draft of this report and requested written comments on the recommendation, which are included in Appendices 1 and 2 and were considered in finalizing the report. As

⁶ National Network To End Domestic Violence, Safety Net Project, [Using Uber: Safety & Privacy Considerations for Survivors](https://www.techsafety.org/s/Using-Uber-Safety-Privacy-Considerations-for-Survivors_2023-0328.pdf), March 2023, www.techsafety.org/s/Using-Uber-Safety-Privacy-Considerations-for-Survivors_2023-0328.pdf (accessed December 2024).

discussed in Appendix 3, based on actions taken by OJP and OWW the status of the recommendation is closed.

If you have any questions, please contact me at (202) 514-3435, or Jason R. Malmstrom, Assistant Inspector General for Audit, at (202) 616-4633.

cc: Iyauta I. Green
Director
Office of Audit, Assessment, and Management
Office of Justice Programs

Melonie Threatt
Acting Team Leader
Audit Coordination Branch
Audit and Review Division
Office of Audit, Assessment, and Management
Office of Justice Programs

Brian Lea
Deputy Associate Attorney General
Office of the Associate Attorney General

Micah Fielden
Senior Counsel
Office of the Associate Attorney General

Jason Manion
Counselor
Office of the Associate Attorney General

Louise Duhamel
Assistant Director
Audit Liaison Group
Internal Review and Evaluation Office
Justice Management Division

Erin Lorah
Associate Director
Grants Financial Management Division
Office on Violence Against Women

Chad Mizelle
Chief of Staff to the Attorney General

Jordan Fox
Chief of Staff to the Deputy Attorney General

James McHenry
Associate Deputy Attorney General

Jolene A. Lauria
Assistant Attorney General for Administration
Justice Management Division

Christopher C. Alvarez
Deputy Assistant Attorney General
Controller
Justice Management Division

Alan Hanson
Director
Appropriations Liaison Office
Justice Management Division

Nikita Prudy
Appropriations Liaison Officer
Justice Management Division

Daniel Lucas
Appropriations Liaison Officer
Justice Management Division

APPENDIX 1: THE OFFICE OF JUSTICE PROGRAMS RESPONSE TO THE DRAFT MANAGEMENT ADVISORY MEMORANDUM



U.S. Department of Justice

Office of Justice Programs


Office of the Assistant Attorney General

Washington, D.C. 20531

August 26, 2025

MEMORANDUM TO: William M. Blier
Acting Inspector General
United State Department of Justice

THROUGH: Jason R. Malmstrom
Assistant Inspector General – Audit Division
Office of the Inspector General
U.S. Department of Justice

FROM: Maureen A. Henneberg 
Deputy Assistant Attorney General

SUBJECT: Draft Management Advisory Memorandum - *Notification of
Concerns Regarding the Need for Grant Recipients to Safeguard
Victim Information When Using Various Technologies*

This memorandum provides a response to the Office of the Inspector General's (OIG) May 22, 2025, draft Management Advisory Memorandum (MAM), *Notification of Concerns Regarding the Need for Grant Recipients to Safeguard Victim Information When Using Various Technologies*.

The OIG recommended that the Office of Justice Programs (OJP) and the Office on Violence Against Women (OVW) “[c]oordinate and take actions to raise awareness among grant recipients on mitigating risks to victim safety that can occur through the use of technologies that store personally identifiable information (PII) and location information.”

As discussed with the OIG, OJP concurs with this recommendation. OJP will continue to coordinate with OVW on issues related to victim confidentiality, including those raised in the MAM. In collaboration with OVW, OJP developed the attached bulletin for Office for Victims of Crime grantees about concerns regarding victim safety that can occur through the use of technologies that store PII and location information and available technical assistance resources. The bulletin was distributed to OVC grantees on August 21, 2025.

If you have questions regarding this response, please contact Iyauta I. Green, Director, Office of Audit, Assessment, and Management, by phone at (202) 820-6807.

Attachment

cc: Katherine Darke Schmitt
Acting Director
Office for Victims of Crime
Office of Justice Programs

Rachel Johnson
Chief Financial Officer
Office of the Chief Financial Officer
Office of Justice Programs

Rafael A. Madan
General Counsel
Office of Justice Programs

Iyauta I. Green
Director
Office of Audit, Assessment, and Management
Office of Justice Programs

Phillip Merkle
Acting Director
Office of Communications
Office of Justice Programs

Louise Duhamel
Assistant Director
Audit Liaison Group
Internal Review and Evaluation Office
Justice Management Division

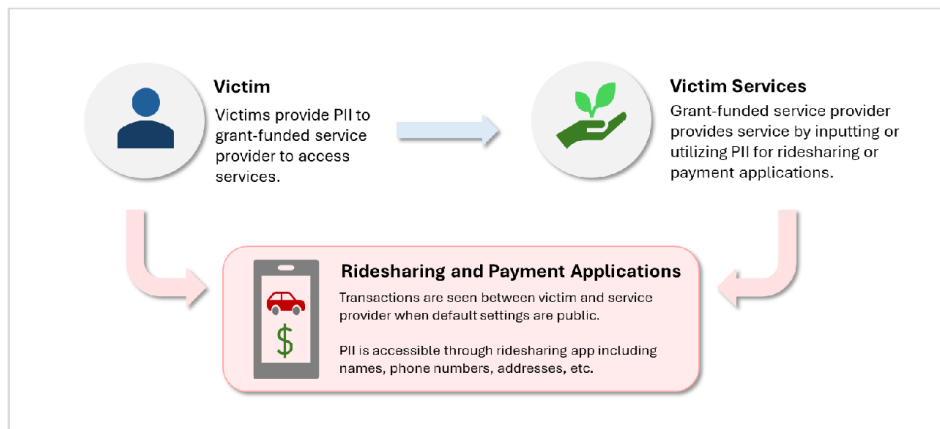
Jorge L. Sosa
Director
Office of Operations – Audit Division
Office of the Inspector General

OJP Executive Secretariat
Control Number OCOM001523

Bulletin

Ridesharing Information for Subrecipients of VOCA and VAWA Funding

Rideshare services can be integral to meeting transportation needs and a valuable resource for victims of crime to receive services. However, the use of rideshare services for victims of crime have raised concerns regarding the lack of user privacy and potential exploitation of data.



According to the [GSA Rules of Behavior for Handling Personally Identifiable Information \(PII\)](#), PII “refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.” PII is also defined in the Violence Against Women Act ([34 U.S.C. 12291\(a\)\(25\)](#)) as “individually identifying information for or about an individual including information likely to disclose the location of a victim of domestic violence, dating violence, sexual assault, or stalking, regardless of whether the information is encoded, encrypted, hashed, or otherwise protected, including--(A) a first and last name; (B) a home or other physical address; (C) contact information (including a postal, e-mail or Internet protocol address, or telephone or facsimile number); (D) a social security number, driver license number, passport number, or student identification number; and (E) any other information, including date of birth, racial or ethnic background, or religious affiliation, that would serve to identify any individual.”

While few State Administrative Agencies (SAAs) provide direct service to victims of crime, all partner with subrecipient agencies that provide varied victim services throughout their state, territory, or Tribe. Subrecipient agencies may offer access to rideshare services, so the Office for Victims of Crime (OVC) and the Office on Violence Against Women (OVW) encourage SAAs to raise awareness of this issue with their state partners.

As of August 13, 2025

Bulletin

Ridesharing Information for Subrecipients of VOCA and VAWA Funding

I. Privacy and Confidentiality Requirements

Numerous state and federal laws protect data privacy and the confidentiality of PII in professional relationships. The U.S. Congress has codified victim confidentiality in the Violence Against Women Act (34 U.S.C. 12291(b)(2)), the Family Violence Prevention and Services Act (42 U.S.C. § 10401), and the Victims of Crime Act (34 U.S.C. § 10101 et seq.). These laws prohibit sharing PII about victims without informed, written, time-limited consent, and they prohibit disclosure of individual information without written consent. Additionally, some (but not all) OJP and OVW awards include measures to address victim confidentiality and privacy, such as requiring written policies to maintain confidentiality and guidance on reporting breaches. SAAs and subrecipients should review their award conditions to ensure compliance with confidentiality and privacy requirements.

II. Raising Awareness

OVC and OVW recognize the importance of raising awareness of safeguarding victim information when using rideshare services with all SAAs and the over 6,000 subrecipients they fund. We encourage SAAs to provide continued notice of these potential risks to their subrecipients through increased education and outreach. Below are some resources that may help in outreach.

[*Using Uber: Safety & Privacy Considerations for Survivors*](#), National Network To End Domestic Violence, Safety Net Project, March 2023.

[*APPLE SAFETY CHECK TIPSHEET*](#), National Domestic Violence Hotline, 2023.

[*National Institutes of Health's National Library of Medicine, "Safeguarding patients from technology-facilitated abuse in clinical settings: A narrative review," PMCID 9931347, January 4, 2023.*](#)

[*Safety Net Project: Exploring Technology Safety in the Context of Intimate Partner Violence, Sexual Assault, and Violence Against Women*](#), National Network to End Domestic Violence, Safety Net Project, 2019.

As of August 13, 2025

APPENDIX 2: THE OFFICE ON VIOLENCE AGAINST WOMEN RESPONSE TO THE DRAFT MANAGEMENT ADVISORY MEMORANDUM



U.S. Department of Justice


Office on Violence Against Women

Washington, DC 20530

September 8, 2025

MEMORANDUM

TO: William M. Blier
Acting Inspector General

FROM: Ginger Baran Lyons 
Deputy Director for Grants Development
and Management (Supervisory Official)

SUBJECT: Response to the Office of the Inspector General's Draft Management Advisory Memorandum, *Notification of Concerns Regarding the Need for Grant Recipients to Safeguard Victim Information When Using Various Technologies*

This memorandum provides a response to the Office of the Inspector General (OIG)'s May 22, 2025, draft Management Advisory Memorandum, *Notification of Concerns Regarding the Need for Grant Recipients to Safeguard Victim Information When Using Various Technologies*. The Office on Violence Against Women (OVW) appreciates the opportunity to review and comment on this memorandum.

The draft Management Advisory Memorandum directed one recommendation to OVW: that the Office of Justice Programs (OJP) and OVW “coordinate and take actions to raise awareness among grant recipients on mitigating risks to victim safety that can occur through the use of technologies that store PII and location information.”

OVW concurs with this recommendation. In coordination with OJP’s Office for Victims of Crime (OVC), OVW has issued a bulletin to State Administering Agencies (SAAs) to raise awareness of threats to victim safety posed by technologies that store PII and location information. In addition, OVW will engage a technical assistance provider to develop a webinar, which will be distributed to SAAs upon completion. Beginning with the next funding cycle, OVW will include this webinar in its new grant recipient orientation materials.

OVW appreciates the opportunity to review and comment on the draft report. If you have any questions or require additional information, please contact Kevin Mihalyi, Senior Audit Liaison, at (202) 717-5696.

cc:

Brian Lea
Deputy Associate Attorney General

Micah Fielden
Senior Counsel

Office of the Associate Attorney General

Jason Manion
Counselor
Office of the Associate Attorney General

Louise Duhamel
Assistant Director
Audit Liaison Group
Internal Review and Evaluation Office
Justice Management Division

Kendra Wharton
Associate Deputy Attorney General

Erin Lorah
Associate Director
Grants Financial Management Division
Office on Violence Against Women

Diane Dauplaise
Attorney Advisor
Office on Violence Against Women

Kevin Mihalyi
Senior Audit Liaison
Office on Violence Against Women

APPENDIX 3: OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS CLOSING THE REPORT

The Office of the Inspector General (OIG) provided a draft of this report to the Office of Justice Programs (OJP) and the Office on Violence Against Women (OVW). OJP's and OVW's responses are incorporated as Appendix 1 and Appendix 2, respectively, of this final report. OJP and OVW concurred with the recommendation and provided sufficient documentation of completed corrective actions. As a result, the status of the report is closed. The following provides the OIG analysis of the responses.

Recommendation for OJP and OVW:

- 1. Coordinate and take actions to raise awareness among grant recipients on mitigating risks to victim safety that can occur through the use of technologies that store personally identifiable information (PII) and location information.**

Closed. OJP concurred with our recommendation. In collaboration with OVW, OJP developed a bulletin for Office for Victims of Crime (OVC) Victims of Crime Act and Violence Against Women Act grantees addressing victim safety concerns related to technologies that store PII and location information and available technical assistance resources. The bulletin was distributed to OVC-funded state administering agencies (SAAs) in August 2025. OJP also stated in its response that it will continue coordinating with OVW on victim confidentiality issues.

OVW concurred with our recommendation, and as described above, coordinated with OJP to develop and distribute a bulletin to SAAs to raise awareness of threats to victim safety posed by technologies that store PII and location information. OVW also stated that it will engage a technical assistance provider to develop a webinar, which will be distributed to SAAs upon completion and be included in its new grant recipient orientation materials.

We reviewed the documentation provided and available publicly, and we determined that it adequately addressed the recommendation. Therefore, this recommendation is closed.