



Eliminating Sensitive Data Leaks

Jeff Rummelsburg

Randall Williams

Esri Software Security & Privacy

ESRI USER CONFERENCE 2024

2024

Pop Quiz



Q: What is the most common security issue reported by users of ArcGIS Online?

a. Denial of Service

b. Information Leaks/Spills

c. “Misinformation Propagation”

d. Hacked Accounts

Q: How do ArcGIS Online information leaks and spills occur?

- a. Organization configuration
- b. Item configuration
- c. Account sharing practices
- d. Lack of governance
- e. All of the above

What do we do about this?

Let's discuss:

- Understanding Sensitive Data & Causes of Data Leaks
- Esri Privacy Initiatives & ArcGIS Online
- Configuration options and best practices
- Tools to help Monitor
- Processes and Pipelines



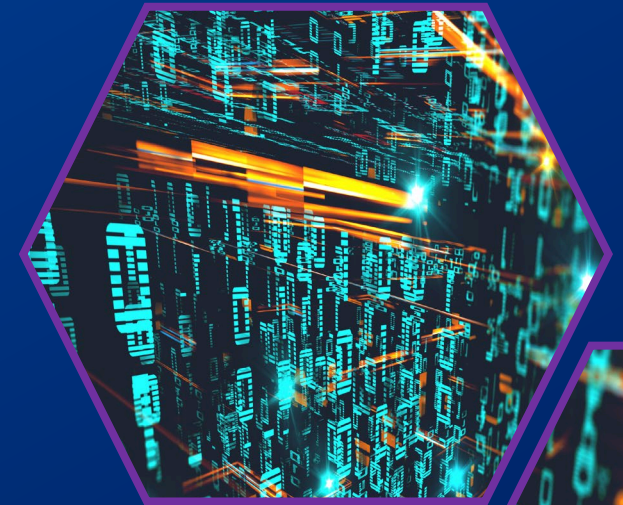
Understanding Sensitive Data & Causes of Data Leaks

What is a Data Leak?

A data leak is the accidental or overlooked exposure of sensitive information.

Data leaks occur when sensitive data is accidentally exposed publicly, either physically or digitally. Common causes of data leaks include:

- Misconfigured software settings
- Accidental Sharing
- Social engineering
- Recycled or weak passwords
- Physical theft/loss of sensitive devices
- Software vulnerabilities
- Insider threats



UpGuard researchers discovered that at least 47 organizations were unknowingly leaking data through a misconfiguration in Microsoft's PowerApp solutions - an oversight resulting in the exposure of tens of millions of private records.

What is Sensitive Data?

Sensitive data refers to any information that, if disclosed, could cause harm to an individual, organization, or entity.



Customer Data

Demographics
Product usage
Customer history
Customer information



Analytic Data

Customer behavior
Modeled data
Psychographic data



Regulated Data

HIPPA
FERPA
PCI DSS



Personal Information

Names
Addresses
Email
SSN



Location Data

Movement patterns
Business locations
Coordinates



Esri Privacy Initiatives & ArcGIS Online



Building a Culture of Privacy

Privacy at its core: Our privacy efforts focus on internal governance systems that integrate privacy and data usage standards throughout Esri's operations.

- + Privacy Committee: A multi-departmental committee, meeting monthly to uphold our privacy commitments.
- + Integration: Privacy is embedded as an essential feature in our processes and development.
- + Accountability & Trust: Shared responsibility of protecting privacy and transparency about data handling practices.
- + Privacy Resources: Internal site and guidance documentation on privacy best practices.

Privacy Education: We advocate that privacy is a collective responsibility and promote ongoing education through training and awareness campaigns.

- + Privacy Training and Awareness
- + Privacy week
- + Roadshows



Esri's Product Privacy Priorities

- + **Designing for privacy:** We design our products with privacy in mind from the start.
 - + Privacy by Design (PbD)
 - + Secure privacy experience
 - + Age-Appropriate Privacy
- + **Building privacy into our processes:** We have processes in place to ensure that privacy is considered throughout the development and operation of our products.
- + **Safeguards & controls:** We've established both procedural and technical measures to mitigate privacy risks, ensuring compliance with all regulatory requirements related to data privacy.
- + **Incident Management:** Our Incident Management program oversees the processes for identifying, assessing, mitigating, and remediating privacy incidents.
- + **Privacy Principles:** Our processes guide the development of new or modified products, services, or practices according to our internal privacy expectations.
 - + Purpose Limitation
 - + Data Minimization & Retention
 - + Data Access & Management
 - + Fairness & Accountability



Esri's Privacy Initiatives in ArcGIS Online

- + **Accountability & Transparency:** We offer customers a Data Processing Addendum (DPA) with privacy commitments, including data transfer mechanisms and provisions for compliance with data protection laws.
- + **Security:** ArcGIS Online offers a variety of privacy features to ensure the security and confidentiality of user data including encryption, coding best practices, access control, and deployment models.
- + **Resources & Guidance:** Extensive customer privacy guidance documents that covers high-level architecture guidance, down to individual configuration settings.
- + **Privacy Rights:** Facilitate compliance with data protection regulations through features for data access, export, deletion, and updates. This includes support for processing restrictions, consent, data portability, and the right to be forgotten.
- + **Privacy Compliance:** Adherence to GDPR, CCPA, and other international data privacy laws
- + **Ownership Retention:** Customers maintain full ownership of their content. This means that the data you upload to ArcGIS Online remains yours.



Future of Privacy & Esri's Commitment

- + **New laws & regulations:** By the end of 2024, it is predicted that 75% of the world's population will have their personal data covered under modern privacy regulations.
- + **Technological Advancements:** The development of privacy software and tools will play a significant role in the future of privacy.
- + **AI Review:** As AI expands, our Responsible AI efforts are driven by our mission to ensure the positive impact of AI for people and society.
- + **Data Localization:** There is increasing attention to data sovereignty issues worldwide.
- + **Prioritize transparency and communication:** Clearly communicate with customers about data collection, usage, and protection measures to ensure trust.

Esri commitment to privacy: Protecting user data and privacy is vital to our business and vision. We continuously enhance our privacy program and products to meet evolving expectations and technological advancements.





Configuration Options & Best Practices

Tons of materials in ArcGIS Trust Center

Papers!

Presentations!

Limiting Access to Public Survey123 Responses

Version 2.0

Esri Software Security and Privacy



An Esri
Software Security and Privacy
Technical Paper

January 2023

Version 3.2

ArcGIS® Location Sharing Privacy Best Practices



esri®

GeoDev Webinar Series

A Guide to Understanding ArcGIS Online Security and Privacy

ArcGIS Enterprise Hardening Guide



AN ESRI
TECHNICAL PAPER

April 2024

ArcGIS Enterprise Hardening Guide

Table 6—MFA Authentication Options

MFA Authentication Type	Basic	Advanced	Effort
Built-In (Multifactor) for Admins	X		Low
Built-In (Multifactor) for All		X	Low
SAML/OpenID Connect	X		Moderate*
Passwordless		X	Moderate
FIDO2 Key		X	High
Certificate/CAC/Smart card		X	High

*Low for organizations with an IDP already in place

Advanced: Configure All User Accounts with MFA

If your organization would be willing to consider one Advanced control, this is the one to implement with the strongest security value for your implementation. Don't be surprised to see this become a Basic control in the next year to two because of the value and criticality of the control. To be clear, this is another prerequisite to support ZTA with ArcGIS Enterprise. This control covers all authentication types covered in Table 6. For SAML or OIDC IDP accounts, ensure you deploy phishing-resistant MFA solutions such as FIDO2 and WebAuthN.

Centralized Identity Management

A production ArcGIS Enterprise implementation should not establish a separate silo of user accounts but instead utilize centralized identity management systems. Built-in ArcGIS Enterprise accounts should be documented as exceptions for specific use cases. Establishing a strong foundation for identities utilized to access systems is a key pillar to advancing the ZTA initiative that subsequently requires authentication and authorization at all exposed system interfaces, eliminating anonymous access to your

Table 11—Alignment of Security and Privacy Principles

Issue/Control	Description	Recommendations
Data Encryption	Data at rest and in transit should be encrypted to protect sensitive information and ensure privacy compliance.	Implement encryption for data at rest using ArcGIS Data Store and use SSL/TLS for securing data in transit.
Authentication and Authorization	Proper authentication and authorization mechanisms are crucial to ensure that only authorized users have access to sensitive data.	Configure and enforce strong authentication mechanisms, such as SAML, OAuth 2.0, or integrated Windows authentication. Set up appropriate user roles and permissions.
Access Logging and Monitoring	Monitoring user activities and logging access to sensitive data are essential to detect potential privacy breaches.	Enable and configure logging within ArcGIS Enterprise components. Implement monitoring and auditing tools for user activities.
Data Minimization	Collecting and processing the minimum amount of personal data necessary reduces privacy risks.	Review data collection practices and ensure that only the necessary personal data is collected and processed.
Privacy Settings for Shared Content	Inadvertent sharing of sensitive data with unauthorized users can lead to privacy breaches.	Configure default sharing settings and provide guidance to users on sharing content securely and responsibly.
Anonymization and Pseudonymization	Anonymizing or pseudonymizing personal data can help reduce privacy risks by limiting the identification of individuals.	Implement anonymization or pseudonymization techniques where appropriate, especially when sharing or analyzing personal data.
Retention and Deletion Policies	Proper data retention and deletion policies should be in place to ensure compliance with	Define and implement data retention and deletion policies in line with local, state, and federal laws.

Cheat Sheets!

<https://TRUST.arcgis.com>

Online & Enterprise

Privacy Guidance Included



Monitor & Validate



Monitor and Validate

*Dear Esri,
It would be super cool if you had a tool that
can tell me if I might have Privacy leaks.*

Love,

Users



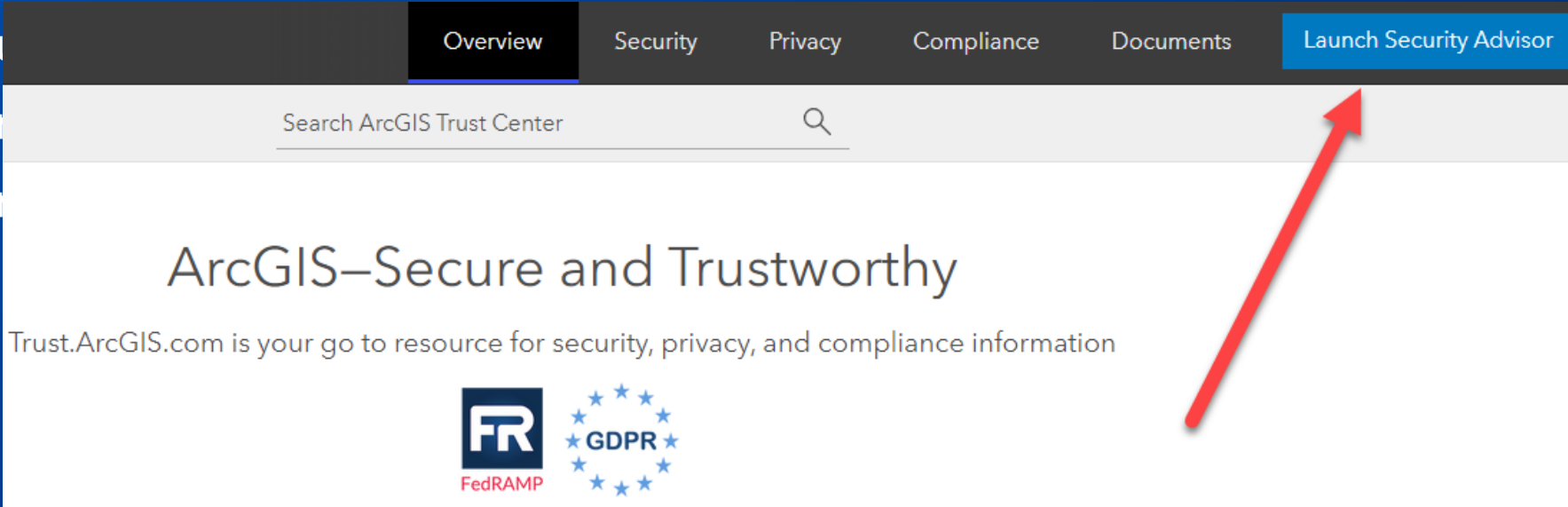
ArcGIS Security and Privacy Advisor!

- Link from ArcGIS Trust Center

- S

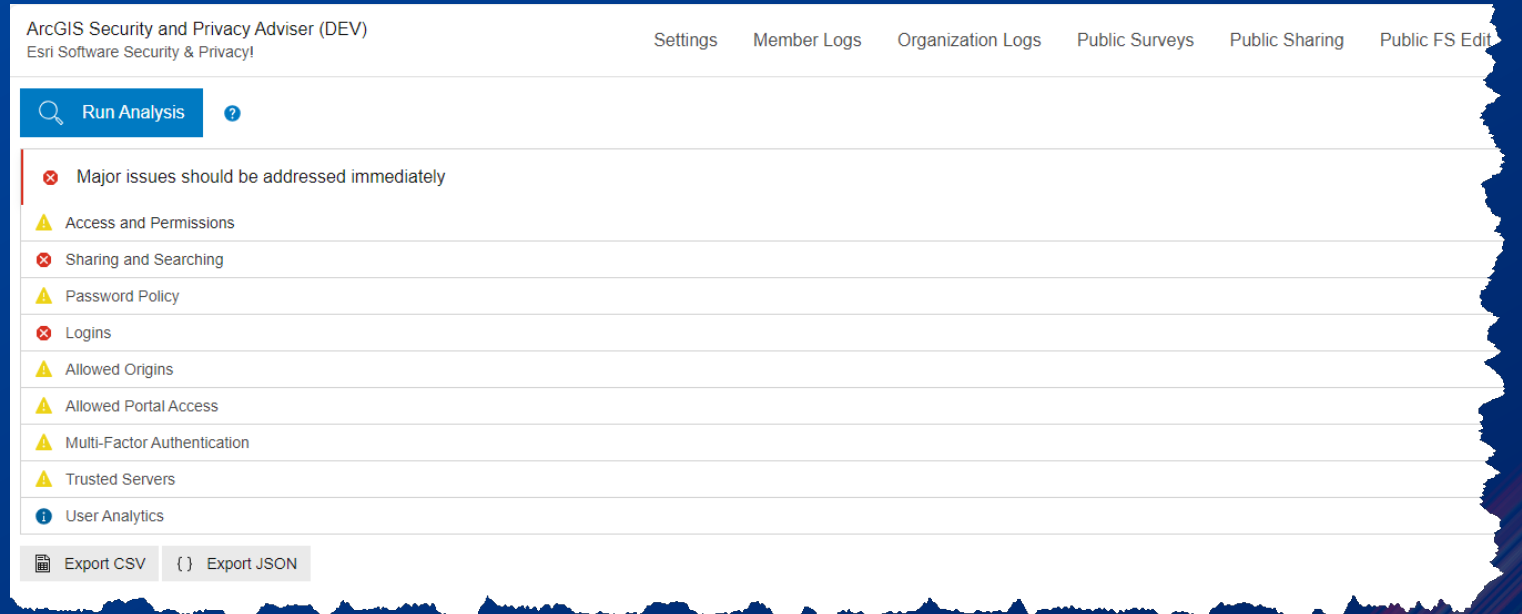
- P

- P



DEMO: ArcGIS Security and Privacy Advisor!

- Validate:
 - Settings
 - Survey Result Visibility
 - Public Items
 - Public Edit capabilities



The screenshot displays the ArcGIS Security and Privacy Advisor (DEV) interface. The header includes the title "ArcGIS Security and Privacy Advisor (DEV)" and "Esri Software Security & Privacy!". Navigation links for "Settings", "Member Logs", "Organization Logs", "Public Surveys", "Public Sharing", and "Public FS Edit" are visible. A search bar contains the text "Run Analysis" with a magnifying glass icon and a help icon. The main content area lists several security issues with corresponding icons: a red 'x' for "Major issues should be addressed immediately", a yellow triangle for "Access and Permissions", a red 'x' for "Sharing and Searching", a yellow triangle for "Password Policy", a red 'x' for "Logins", a yellow triangle for "Allowed Origins", a yellow triangle for "Allowed Portal Access", a yellow triangle for "Multi-Factor Authentication", a yellow triangle for "Trusted Servers", and a blue 'i' for "User Analytics". At the bottom, there are buttons for "Export CSV" and "Export JSON".

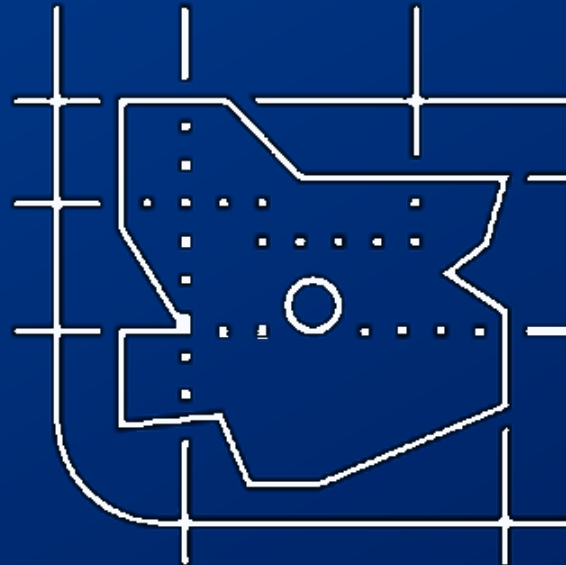


Processes & Pipelines To Govern Information Delivery

Real Risks the Wild

Privacy Leaks: School Bus Stop Geocoding/Routing

#1 Reported Privacy issue to Esri PSIRT – STUDENT PII/PHI



Real Risks the Wild

Privacy Leaks: Public Survey Results...

...Misconfigured Surveys?

Proprietary Data Sets: Public Sharing...

...Contractors?

Product Improvements Implemented!
Technical Documents Written!



WHAT'S MISSING...?

Customer Responsibilities

Processes

- Establish a content Publication Review Board
 - Review content before publication
 - Regularly review content after
 - **Disable the ability for users to share publicly**
- Classify your datasets and secure them appropriately
 - Leverage groups to bucket datasets
 - Use tags to label data
 - Create groups to share sensitive data with
 - Limit access to groups
- Use custom roles to granularly define permissions
 - Don't use ADMIN as daily driver



PROCESSES

Customer Responsibilities

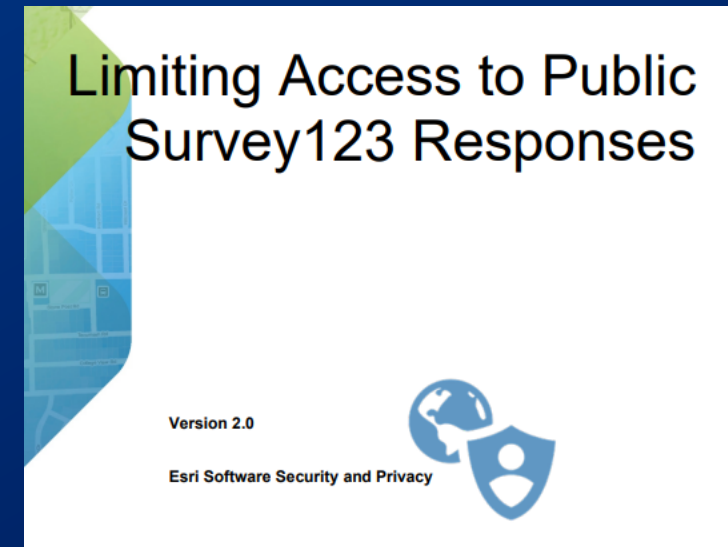
Processes

- **REVIEW ALL CONTENT PRIOR TO SHARING TO “EVERYONE”**
- Enable and use Multi Factor Authentication
- Leverage Hosted Feature Service Views
- Filter sensitive content
- Delete sensitive columns before publishing (as feasible)
 - POP UP FILTERING is NOT ENOUGH!
 - (Client-Side filtering does NOT prevent direct queries to web service)

Technical Papers in ArcGIS Trust Center



PROCESSES





esri[®]

**THE
SCIENCE
OF
WHERE**[®]

Copyright © 2024 Esri. All rights reserved.