An Esri
Software Security and Privacy
Technical Paper

January 2023

Version 3.2

ArcGIS® Location Sharing Privacy Best Practices

380 New York Street
Redlands, California 92373-8100 USA
909 793 2853
info@esri.com
esri.com

esri® THE SCIENCE OF WHERE™

Contents

1 Introduction

Enterprise geographic information system (GIS) deployments have increasingly incorporated location sharing information that require adherence to advancing privacy regulations. This makes deployments more complex and challenging for information technology (IT) architects and privacy specialists to deploy an effective enterprise GIS security strategy. However, privacy principles and controls stemming from regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) can be applied at all levels of the ArcGIS system architecture to ease this effort, including location sharing.

Be aware that clear, open communications with your user base (being monitored via location sharing) is an absolute necessity. Transparency with the users can help ensure that privacy obligations are met and foster stronger trust of the user base, resulting in broader uptake of tracking solutions and benefits (see section 2.2) to your organization. This includes providing details concerning what users can control at the mobile app level and any of the devices being deployed around them, such as beacons or receivers.

This document contains relevant information that helps guide IT managers, GIS administrators, and privacy and security team members in deploying cloud and enterprise GIS in a manner that helps comply with privacy regulations, such as GDPR, for location sharing services. Though GDPR is specifically for information sets related to individuals within the European Union, in the process of addressing these privacy requirements, your organization is well on its way to meeting its privacy needs independent of industry or location. This paper discusses several different deployment scenarios along with some privacy considerations. The objective is to provide users with background, guidance, and answers to frequently asked questions (FAQs) regarding privacy as they implement the ArcGIS® platform with location sharing capabilities. This is not legal advice or intended to be used as certification of compliance with any privacy law or regulation.

2 Background

Location sharing services are important because they provide real-time operational awareness for the field, which aids in improving worker efficiency and safety. Some use cases for location sharing services are disaster relief, utilities services for validation of proof of work, law enforcement for improved situational awareness, and large events such as marathons and parades. Location sharing can afford opportunities to save lives by tracking work to verify and allow for better public safety[1]. The default accuracy levels of most location collection technologies today create datasets that fall under privacy and compliance regulations. Therefore, this section provides additional context concerning privacy obligations, what location services are, the supporting technologies of ArcGIS Online and ArcGIS Enterprise, and the specific Esri® applications that can be utilized with location sharing services today.

2.1 Privacy and Compliance

Esri values the privacy of its customers, distributors, and partners, as it is a principal component of establishing trust. Esri has created a general company Privacy Statement and a separate Products & Services Privacy Statement Supplement to ensure that customers receive the level of privacy they deserve and expect. These privacy statements describe how Esri collects data and uses information you provide to us and are independently validated.

With the deprecation of the EU-US Privacy Shield Esri implemented the EU and UK Standard Contractual Clauses (SCC's), and supplementary security measures regarding the collection, use, and retention of personal information transferred from the European Union, Switzerland, and the United Kingdom to the United States. Esri is a processor of personal information for other controller organizations (i.e., our customers) who have entrusted us with processing personal information that they control. Esri's location sharing software and services allow customers to comply and fulfill the regulatory requirements of GDPR and CCPA.   Esri has a Data Processing Addendum (DPA) available for signing that sets the conditions related to privacy, confidentiality, and security of personal data associated with online services and maintenance that we provide to customers under a master agreement.

What Is Personally Identifiable Information?

Privacy is the right to be left alone, or freedom from interference or intrusion. According to the International Association of Privacy Professionals (IAPP), information privacy is the right to have some control over how your personal information is collected and used. Privacy focuses on the use and governance of data, such as the policies and procedures in place to ensure that consumer personal information is being collected, shared, and used appropriately. Security focuses on protecting the personal data from exploitations.

Personally identifiable information (PII) consists of any data that could potentially be used to identify a person. Examples of information that qualifies as PII, according to NIST 800-122, include full name, Social Security number, driver's license number, home address, login information, screen name, passport number, and email address. Under CCPA "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household and it specifically includes online identifiers, internet protocol address and geolocation data. GDPR defines personal data as any information related to a person that can be used to directly or indirectly identify them, examples of which are shown in figure 1 below.

[1] See ArcGIS Tracker, Pasadena Fire Department use case for the 2019 Rose Parade.

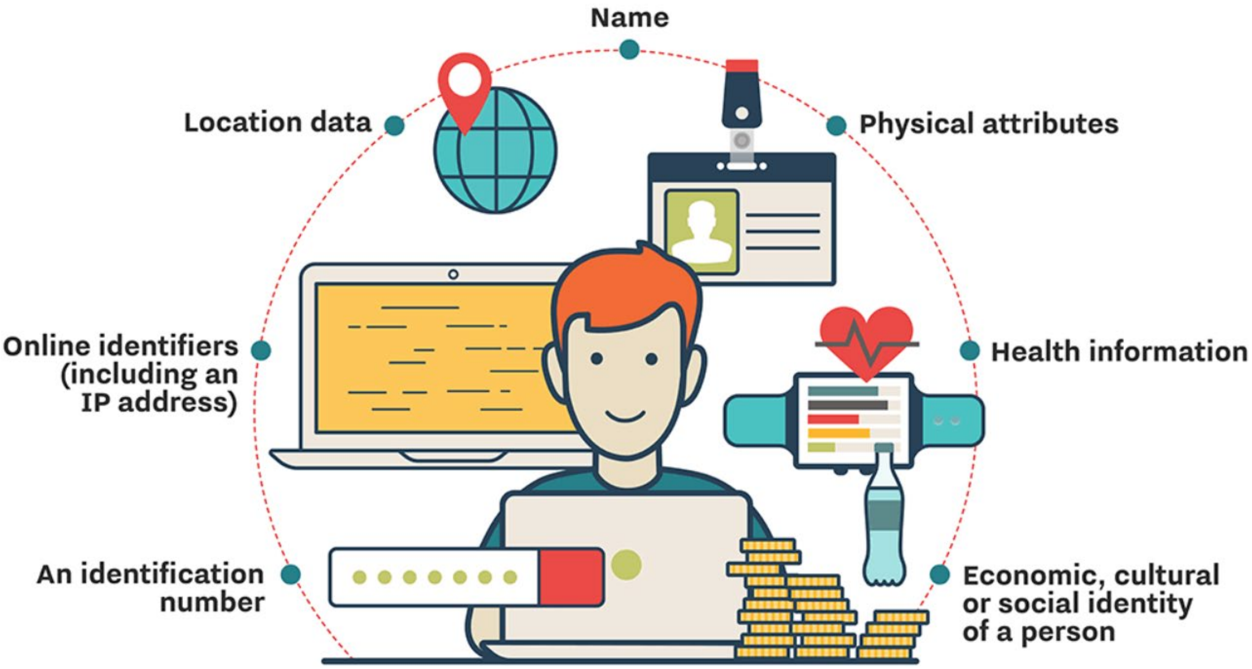

Name
Location data
Physical attributes
Online identifiers (including an IP address)
Health information
An identification number
Economic, cultural or social identity of a person

Figure 1—General Data Protection Regulation (GDPR) Personal Data Examples[2]

Collecting geolocation information for location sharing with a Global Positioning System (GPS) receiver (fine-grained location information) could qualify as PII, as it can lead to reasonable inference of the individual. "Fine-grained location" information for analytics is commonly defined as any area less than one square mile[3], including any spatial (latitude-longitude) data. Other items commonly considered personal data utilized with location services include name, surname, user name, email, IP address, location, and even the advertising identifier of the user's phone.

There are plenty of variances concerning what is personal data between regulations, so a good starting point for identifying PII and understanding its relative risk in your operations is to refer to organization guidance like the IAPP, which provides a PII risk matrix of what is considered high-, medium-, and low-risk PII. Location information by itself is categorized as moderate risk in the matrix, but when combined with a person's first and last name, it is considered high-risk PII. This means the relative PII risk for your location sharing services can be lowered based on the information you choose to process and store.

Esri is an active member of the IAPP and has Certified Information Privacy Technologists (CIPT) within our Software Security & Privacy team to help ensure alignment with current privacy obligations in our products and services.

Because GDPR plays a central role relative to ensuring that privacy concerns are appropriately addressed by organizations today, it is important that you are familiar with key terms such as Data subject, Personal data, Data controller, Data processor, and Service Provider (see Section 10 for definitions). Additional details concerning the privacy of your data with Esri products and our associated compliance information may be found within the ArcGIS Trust Center.

[2] See https://searchdatamanagement.techtarget.com/answer/What-is-included-in-the-GDPR-definition-of-personal-data.

[3] See Google best practices for avoiding sending geolocation PII.

2.2 Location Sharing

A major benefit of location sharing services and applications provided by Esri is that the customer fully owns their data being collected and Esri does not sell or share the data to third parties. Customers are encouraged to compare the strong privacy assurance found in Esri Products & Services Privacy Statement Supplement against other vendor privacy policies. Many other location sharing and tracking solutions utilize customer data to provide targeted marketing of new services and third-party advertising. They also frequently provide customer data to third parties that analyze location and movement trends that might be devoid of personally identifiable information but could potentially be associated directly with a customer's organization. Customers don't have these surprise headaches with the ArcGIS system.

Esri offers location sharing services through both ArcGIS Online (discussed in section 2.3) and ArcGIS Enterprise (discussed in section 2.4). The location sharing service stores data in two or three feature layers:

- Last Known Location (LKL) layer
    - Stores last known location for each mobile user
    - Useful for situational awareness use cases
- Tracks layer
    - Full historical tracks of where each mobile user has been
    - Useful for analysis use cases
- Track Lines layer
    - Full historical tracks for each user displayed as lines
    - Useful for visualization
    - Only supported in ArcGIS Online

The last known location and tracks layers have identical schema, including attributes for activity (iOS Core Motion, Android DetectedActivity), altitude (meters), battery percentage, battery state, created date, and user (used by ownership-based access to determine who can see which tracks), course, floor, level_id, horizontal accuracy (meters), last edited date, last edited user, location time stamp, speed (meters per second), vertical accuracy (meters), session ID, signal strength, category, and device ID. Additional details can be found in the Track layers documentation

2.3 ArcGIS Online

ArcGIS Online is a web-based GIS, hosted by Esri and delivered as a software-as-a-service (SaaS) solution (see figure 2). With ArcGIS Online, organizations can get up and running quickly and securely create, organize, and manage geographic information within one system. It connects users in the organization with up-to-date content, including ready-to-use apps, maps, 3D scenes, and layers, so they can build useful information products and accomplish their work more efficiently. It facilitates collaboration and sharing of information with internal stakeholders, customers, contractors, and the public by providing access to maps, apps, and data from any device, anywhere, anytime. ArcGIS Online is built on open, scalable technology that automatically adjusts to meet peak demand periods. ArcGIS Online is Federal Risk and Authorization Management Program (FedRAMP) Tailored Low SaaS, authorized by the United States government for sharing information with the public. Many organizations with stringent security demands utilize ArcGIS Online as part of a hybrid deployment by using it with their own secure ArcGIS Enterprise systems. Organizations around the world utilize ArcGIS Online as the FedRAMP security standards map to ISO 27001 security controls. Though the ArcGIS Online cloud infrastructure is located within the United States, Esri is Privacy Shield certified, which meets EU adequacy requirements. ArcGIS Online is also GDPR aligned.

GDPR roles for ArcGIS Online are as follows:

- The customer utilizing ArcGIS Online is the data controller.
- The individual to whom personal data relates is the data subject.
- Esri operates as a data processor.
- The cloud services providers are data sub-processors.

For customer assurance purposes, Esri ensures that the data sub-processors handle information appropriately by validating a DPA is in place with each provider.

Figure 2—ArcGIS Online Software as a Service (SaaS)

If you utilize ArcGIS Online as part of your GIS, then it is important that you understand how that impacts your responsibilities under GDPR and other industry and privacy requirements applicable to you. Esri and our sub-processors provide both technical and contractual measures to enable you to meet your GDPR requirements while allowing us to address those requirements for our own operations. If you choose to store personal data in the ArcGIS system, then you remain responsible for that data and how it is managed and used within the system. ArcGIS is a powerful platform for helping with the task of managing personal data and provides tools and capabilities that can address some of the specific requirements of GDPR.

2.4 ArcGIS Enterprise

ArcGIS Enterprise is the software offering from Esri that enables an organization to use the Web GIS pattern as managed services, the cloud environment, and on-premises solutions. It offers a flexible deployment model, allowing use that is completely on-premises; connected or disconnected from the internet; on physical hardware or in virtualized environments; in the cloud on Amazon Web Services (AWS), Microsoft Azure, or any cloud platform that provides virtual machines that meet the system requirements and specifications; or as an Esri managed service.

GDPR roles for ArcGIS Enterprise are as follows:

- The customer managing ArcGIS Enterprise is the data controller.
- The individual to whom the personal data relates is the data subject (such as the individual recording and sharing locations with ArcGIS Field Maps).

Unlike ArcGIS Online, Esri typically does not have a direct role with personal data when using ArcGIS Enterprise because the software is installed and managed on the customer premises. The customer has full control over the deployment.

2.5 Data Sources

Location-based technology has found its way in a variety of applications today such as wireless location services GIS technology. ArcGIS location-based services (LBS) have several options (see figure 4), which can be used as data sources such as beacons, Wi-Fi, and internal and external GPS. Typically, mobile devices are configured to utilize a combination of these data sources, which can then be stored by ArcGIS location sharing services, if desired. This section provides an overview of mobile device location-based services (additional details concerning privacy, spoofing concerns, and countermeasures for various data sources are discussed in section 8.2).

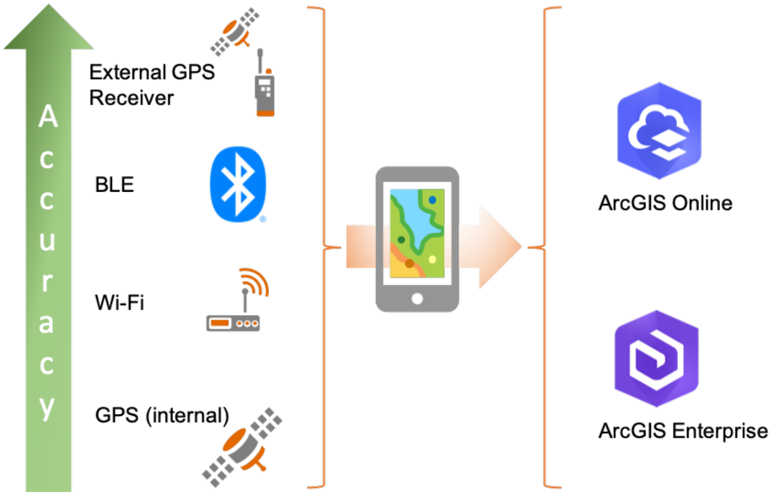


Figure 3—Common Data Sources for Location-Based Services

Mobile Device Location-Based Services

Location services utilize GPS and Bluetooth (where available), along with crowdsourced Wi-Fi hot spot and cell tower locations, to determine a device's approximate location. By enabling location services for your devices, you agree and consent to the transmission, collection, maintenance, processing, and use of your location data and location search queries by Apple/Google and their partners and licensees to provide and improve location-based and road traffic-based products and services.

Android devices support four location modes: high accuracy, battery saving, device/sensor only, and off. The high accuracy mode generally provides the best location accuracy by using a combination of GPS, Wi-Fi, Bluetooth, and mobile networks. Since applications which utilize location sharing (e.g. ArcGIS Field Maps, ArcGIS QuickCapture & ArcGIS Indoors) efficiently request locations and minimize impact on battery life, you can use high accuracy mode and get the most accurate locations. Apple iOS Location Services may be turned on or off and uses GPS and Bluetooth (where those are available) along with crowd-sourced Wi-Fi hotspot and cell tower locations to determine your device's approximate location.

If you allow Esri apps, such as ArcGIS Field Maps, ArcGIS QuickCapture & ArcGIS Indoors or websites, to use your current location, you are subject to Esri's terms, privacy statement, and practices. In addition to this document, please see the ArcGIS Trust Center Documents and Privacy sections to further understand Esri's privacy commitments.

2.6 Applications

This paper focuses primarily on the location sharing capability which is used by ArcGIS Field Maps, ArcGIS QuickCapture and also touches on the ArcGIS Indoors™. These apps are designed to write tracks to Esri's location sharing services provided by ArcGIS Enterprise and ArcGIS Online. Other ArcGIS applications, such as Map Viewer, have been engineered to read the track information created.

The overall Location Sharing solution includes the following components:

- End-user apps for enabling Location Sharing and viewing
- Professional apps and tools for viewing/sharing tracks and creating feature service views
- Location services backend infrastructure

2.6.1 ArcGIS FieldMaps

ArcGIS Field Maps (see figure 4) is a mobile solution that provides a map centric mobile experience, that enables users to view, capture and edit spatial data. ArcGIS Field Maps, available for Android and iOS, can share location efficiently whilst the app runs in the foreground or the background. ArcGIS Field Maps can capture last known locations with or without a data connection, and directly share these as points and tracks to a Location Sharing service when connected.

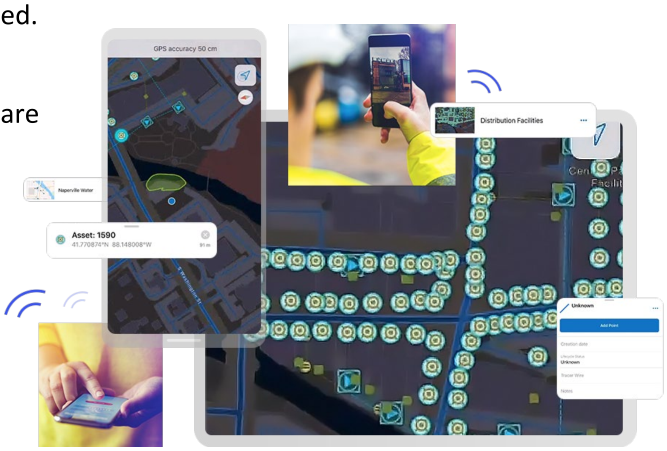


Figure 4—The ArcGIS Field Maps Interface

Using Track Viewer and/or other applications such as ArcGIS Dashboards, organizations can monitor where mobile teams are and analyze where they have been. With this comprehensive view of location patterns, decision-makers gain real-time information that supports critical field activities.

Note: A track is a trail of the highlighted lines on the map used to determine where the mobile users are currently or where they have been at a given point in time.

The location sharing feature service stores tracked locations as features in ArcGIS. Administrators can use Track Viewer web app to manage the security of location tracks, allowing customer-authorized[4] users to see last-known locations and location tracks for other users.

[4] Users with the View location tracks content privilege can open Track Viewer and use it to visualize and interrogate tracks.

2.6.2 ArcGIS QuickCapture

ArcGIS QuickCapture (see figure 5) is a mobile solution focused on a rapid data capture experience. Within ArcGIS Quick Capture location sharing can be enabled to provide the ability to record where users are and where they have been. Tracks and last known locations are uploaded from the QuickCapture mobile app to the Location Sharing service. QuickCapture records tracks whether or not there is a data connection and can provide mobile workers with control of when they are and are not tracked.

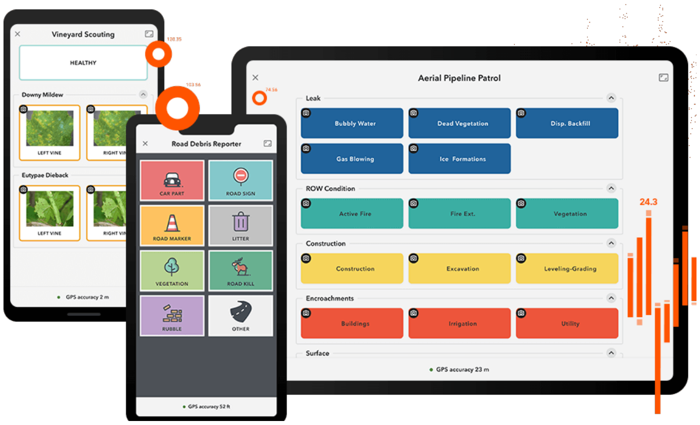


Figure 5—ArcGIS QuickCapture

2.6.3 ArcGIS Indoors

ArcGIS Indoors (see figure 6) supports indoor mapping with the ability to create and share indoor maps and location data. Indoors helps empower employees, occupants, and visitors to make the best use of buildings.

With Indoors, people can be provided a common picture of the environment within and around buildings. Indoor maps let users quickly find people, spaces, and events on-site. Operational data can be incorporated to help effectively maintain facilities, improve safety and security, and better allocate and manage resources.

Figure 2—ArcGIS Indoors Location Concept

The overall Indoors solution includes the following components:

- An extension to ArcGIS Pro to curate and manage indoor data and author floor aware maps.
- A web application template, Indoors Viewer, for way finding and workspace reservation.
- A web application template, Indoors Space Planner, for space management.
- A native mobile (iOS and Android) application, Indoors Mobile, that supports way finding, workspace reservation, and location sharing

3 Architecture

This section provides additional information concerning ArcGIS user terminology, common security components, pros and cons of various location services backend infrastructure configurations, and the architecture components of the applications which provide location sharing capabilities and concludes with privacy and security considerations spanning these offerings.

3.1 ArcGIS User Terminology

Organizations can use, create, and share a wide range of geographic content, including maps, scenes, apps, and layers. The ability of individual organization members to access and work with content in different ways depends on the privileges they have in the organization. User types are a licensing mechanism that allows organizations to control the scope of privileges and capabilities that can be assigned to members through roles.

User Types

Members are assigned a user type when they are invited to an organization as part of the ArcGIS *licensing* model. Some products and capabilities utilize standard user types for licensing; and others, such as location sharing, require an add-on app or User Type Extension license.

User Roles

In addition to a member being assigned a type when they are invited to an organization, they are also assigned a role. A role defines the set of *privileges* assigned to a member. Privileges are assigned to members through either a default role or a custom role. Note that a member's user type (the licensing assigned) determines the default roles that can be assigned to them.

User Privileges

Privileges allow organization members to perform different tasks and workflows in an organization. For example, some members have privileges to create and publish content, while others have privileges to view content but cannot create their own. Privileges are grouped into two main categories:

- **General:** Allows members who perform specific tasks within the organization to work and share with groups, content, and features
- **Administrative:** Allows custom roles to assist the default administrators with managing members, groups, and content in the organization

3.2 Security Components

Segmentation of infrastructure components is recommended for production operations and wherever your organization stores sensitive information, such as PII. Isolating parts of the system limits damage if someone, whether an insider or outsider, breaks into a system or misuses it. Many organizations utilizing ArcGIS applications segment their infrastructure into general tiers (see figure 7) as follows:

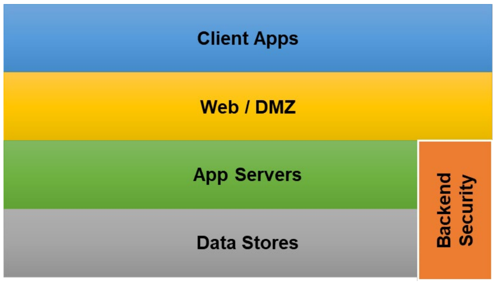


Figure 3—Generalized Infrastructure Segmentation

- **Client Apps:** Main interfaces that users interact with:
    - Browsers, mobile apps, or thick client desktop apps
- **Web/Demilitarized Zone (DMZ):** Middle ground between internal and external systems:
    - Web servers, reverse proxies, and load balancers
    - Bastion host
    - Web application firewall (WAF)
- **App Servers:** Esri applications such as Portal for ArcGIS and ArcGIS Server
- **Data Stores:** Database management systems, ArcGIS Data Store, and file servers
- **Backend Security:** Components frequently leveraged across applications for increased security:
    - Key management system (KMS)
    - Certificate authority (CA)
    - Security information and event management (SIEM)
    - Centrally managed user store (Active Directory/LDAP/IdP)
    - Data loss prevention (DLP)/Data categorization

Note: This section is not meant to be an all-encompassing list of security strategies for an enterprise; some items outside the scope of this section include the following:

- Guidance for isolating environment types, such as production operations versus your development infrastructure, as described in the *Architecting the ArcGIS System: Best Practices* technical paper.
- Evolving security defense postures, such as zero trust, where it is not assumed that actors, systems, or services operations within a security perimeter should be automatically trusted, and instead must verify anything and everything trying to connect to systems before granting access.

Privacy regulations today require that organizations be able to demonstrate a secure posture. Context is provided below for key security components your organization likely has available and which you should utilize as part of your secure ArcGIS deployment. These components can be utilized for both on-premises deployments and those in the cloud. For cloud-based deployments, you may want to make use of the provider's native corresponding security services to meet these needs.

Bastion Host

As an enterprise increases the number of server systems it manages, limiting the number of remote administrative end points exposed, becomes increasingly important. A bastion host provides a consolidated location for allowing administrative access (such as with Secure Shell [SSH] or Remote Desktop Protocol [RDP]), which can typically be security hardened more than application servers. Some of the benefits provided by a bastion host include

- Single point of login to the network for administration, making firewall rules simpler.
- Protection against port scanning by rogue or malicious users outside of your internal network.
- Slowing down potential attackers.

If your organization has use cases requiring GIS administrators to manage GIS resources while outside of an organization's trusted environment, then all connections to these resources should be routed through a bastion. Multifactor authentication (MFA) should be enforced for bastion systems due to their critical nature. Lastly, consider just-in-time bastion access as a defense-in-depth mechanism.

Web Application Firewall

While bastions help protect administrative interfaces, a web application firewall can help reduce successful attacks through your web-based applications such as ArcGIS Enterprise. While Esri has a secure development life cycle to help minimize vulnerabilities at the application level, new exploit techniques can result in vulnerabilities that will need to be patched. A WAF can limit access to the ArcGIS Enterprise administrative APIs, block known exploit patterns, and operate as a temporary patching system if a system cannot be immediately updated with a security patch.

Esri recommends utilizing the Open Web Application Security Project (OWASP) ModSecurity Core Rule Set as a starting point for standardized filtering and adding to the rules over time. If you are utilizing cloud infrastructure, these standardized rules are now just a click away in both Microsoft Azure and Amazon Web Services. Esri's Software Security & Privacy team has provided more detailed implementation guidance for the OWASP rules with ArcGIS Enterprise within the ArcGIS Trust Center documents – Be aware, it is not unusual for some rule adjustments to be made for your organization's specific needs.

Customers desiring a higher level of security assurance beyond the Internet filtering capabilities of a WAF for mobile clients connecting to ArcGIS Enterprise, typically consider Virtual Private Network (VPN) solutions.

Key Management System

KMS ensures proper management of cryptographic keys and secrets (such as passwords) within the organization. KMS truly protects the keys of an organization's kingdom but is commonly implemented with nowhere near the rigor it requires to do it well. Ideally, you consider an implementation that addresses the full life cycle of your keys including such distribution functions as generating, exchanging, storing, using, and replacing keys in operations instead of storing them on administrative/user machines. A key management system can be software or hardware based, and if you are using cloud services, such as Amazon Web Services or Microsoft Azure, you should leverage AWS-KMS services or Azure Key Vault for life cycle management of your encryption keys.

Certificate Authority

This is the entity within or outside your organization that is responsible for issuing digital certificates that may be used for facilitating encryption of data in transit as well as at rest. By default, ArcGIS Enterprise provides a self-signed Transport Layer Security (TLS) certificate to get users up and running quickly with encryption of data in transit. Esri recommends using valid signed certificates instead of self-signed TLS certificates for nonrepudiation and confidentiality in your GIS deployment. For ArcGIS Online, a Security Assertion Markup Language (SAML) signing certificate is provided to the client in the service provider metadata when setting up enterprise logins, and this certificate is renewed every two years.

Security Information and Event Management System

This is a software solution that aggregates and analyzes activity from many different resources across your entire IT infrastructure. It helps ensure alignment with privacy requirements such as the "rights to be forgotten" requirement under article 17 of GDPR, which can be satisfied through the SIEM or similar capability. Deletion of data can be logged as evidence that the user's request to delete all their data was honored.

Importing all ArcGIS application logs into a SIEM is typically a low return proposition, as over 99 percent of the log information is not security related; therefore, Esri recommends that key security events be incorporated from our software applications into the SIEM. To supplement the application security event information logged, we recommend also collecting the web service logs for supplementing identification of patterns. Reach out to our software security and privacy team if you would like to obtain a preliminary list of ArcGIS application security log codes that can be ingested by the SIEM, and then flag or have the SIEM report on these as they occur. The list of the security codes will be added to the customer accessible portion of the ArcGIS Trust Center document repository later this year.

Centrally Managed User Store (Active Directory/LDAP/IdP)

Esri products can leverage Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) as a user store, whether deployed in the cloud or on-premises. However, unlike ArcGIS Enterprise, ArcGIS Online has no direct connection to an LDAP or Active Directory server. For information on how to configure LDAP/AD with ArcGIS Enterprise, please refer to setting up ArcGIS with Active Directory or LDAP. Be aware that user stores typically contain a significant amount of PII, and therefore, appropriate access control measures are required. Esri supports and recommends customers' encrypting the connection from ArcGIS Enterprise to the organization's LDAP/AD. Customers should avoid utilizing separate built-in user account storage for each of their applications; utilizing a centralized user account store is strongly recommended for privacy and security assurance.

Note: The ideal solution for identity management to support both ArcGIS Enterprise and ArcGIS Online users is to rely on the enterprise logins (SAML) option. The advantage of setting up enterprise logins is that members do not need to create additional logins within the ArcGIS Online system; instead, they can use the login that is already set up within their enterprise system and their password does *not* need to be stored within ArcGIS Online. The enterprise login option requires an identity provider (IdP) that is SAML 2.0 compliant, and Esri supports most SAML 2.0 identity providers. Details on how to configure ArcGIS Enterprise or ArcGIS Online for enterprise logins (SAML) as well as the supported IdPs can be found in the ArcGIS Online help.

Data Loss Prevention/Data Categorization

Being able to identify where PII ends up within your operations is a key component of your privacy obligations and mitigating its associated risk. While a data loss prevention system can help identify information sets scattered throughout your organization and what information types are being consumed externally, a good starting point is having at least a component that categorizes data at key locations. When utilizing an enterprise geodatabase with Microsoft SQL Server, you can employ the database's data discovery and classification capabilities to flag PII that may be incorporated with your geospatial datasets. Similar data categorization solutions are offered within cloud services providers.

Esri is looking into the feasibility of alerting a customer's administrator when information identified as potential PII is published as part of a public web service. We recommend considering similar alerting mechanisms utilizing third-party components for your ArcGIS deployments.

3.3 Location Sharing Backend Infrastructure

The foundation of location sharing services is built into both ArcGIS Online and ArcGIS Enterprise. This section provides a brief overview of pros and cons relative to meeting security and privacy requirements when using ArcGIS Online and/or ArcGIS Enterprise deployments. Before choosing a deployment pattern, it is worthwhile to weigh the benefits and drawbacks of each pattern. The deployment patterns to be discussed are below:

- ArcGIS Online
- ArcGIS Enterprise—Single machine
- ArcGIS Enterprise—Multimachine
- ArcGIS Enterprise—High availability

3.3.1 ArcGIS Online

In this configuration pattern, shown in figure 8, the system infrastructure is managed by Esri in alignment with FedRAMP Tailored Low authorization requirements. Key items that a customer is responsible for are organization configuration settings (see Security & Privacy Advisor tool for recommendations and section 8.1), client-side security, categorization of data, privacy assessment, backup of customer datasets, periodic public content checks, and identity management infrastructure via SAML.

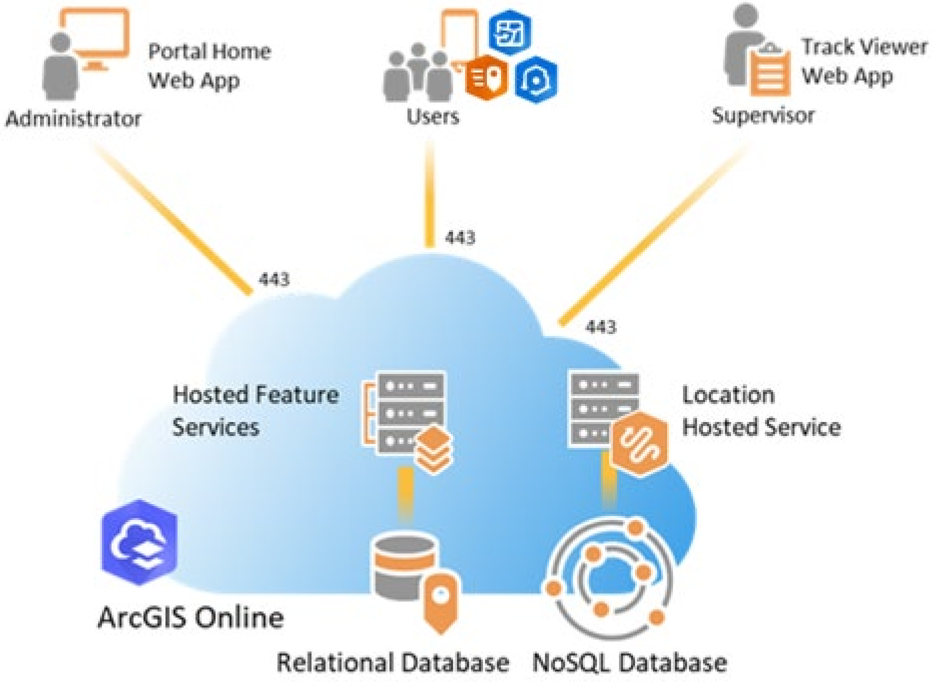


Figure 4—ArcGIS Clients and ArcGIS Online Services Utilized

Advantages

- FedRAMP Tailored Low Impact Software as a Service (LI-SaaS) authorization[5] for US-based operations
- Data encrypted automatically at rest (AES-256) and in transit (TLS 1.2 via port 443)
- No infrastructure administrative overhead since it is leveraging Esri's cloud SaaS
- Highly available solution—multiple active-active data centers
- Data can be hosted in the United States, Europe, or Asia-Pacific regions
- Can be started up in a few minutes

Disadvantages

- FedRAMP authorization does not specify assurance for highly sensitive data or address industry specific requirements such as HIPAA (Note FedRAMP Moderate authorization is expected in 2023)

Recommendations

ArcGIS Online is ideal for publicly accessible data and content or where customer content is not determined to be highly security sensitive. Customers with more highly sensitive data frequently implement a hybrid approach with ArcGIS Enterprise (until FedRAMP Moderate is in place). When utilizing ArcGIS Online, ensure that you periodically assess the security posture of your implementation utilizing the Security Advisor tool; doing so provides evidence that your organization takes active steps to validate the security of PII potentially stored within ArcGIS Online.

3.3.2 ArcGIS Enterprise Components

ArcGIS Enterprise consists of four main deployment components, as shown in figure 9:

- **ArcGIS Web Adaptor:** Installs in a third-party web server, operates as a reverse proxy
- **Portal for ArcGIS:** Front-end user interface for mapping, data management, and sharing
- **ArcGIS Server:** Enables GIS data and content to be shared as web services
- **ArcGIS Data Store:** Managed database storing hosted data

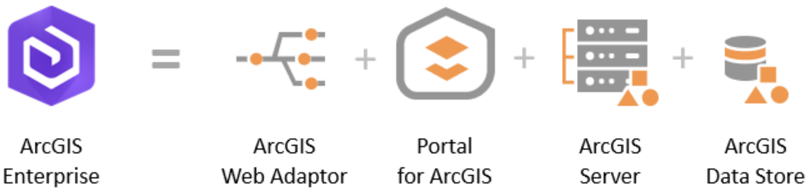


Figure 5—ArcGIS Enterprise Components

These four components can be deployed in diverse combinations and patterns to support many different business workflows. In terms of security, both the Portal for ArcGIS and ArcGIS Server components can support separate security models or share the same security model in a federated deployment.[6]

[5] A FedRAMP (LI-SaaS) authorization provides a minimum set of security control requirements that must be met.
[6] Find more information on federated deployments.

3.3.3 ArcGIS Enterprise—Single Machine

In this configuration pattern, shown in figure 10, all ArcGIS Enterprise components are installed on one machine. You can use the ArcGIS Enterprise Builder or the ArcGIS Cloud builder (AWS & Azure) to simplify deployment. The single-machine deployment components include ArcGIS Server, Portal for ArcGIS, ArcGIS Data Store, and two installations of ArcGIS Web Adaptor (one installation for traffic to your ArcGIS Enterprise portal and one for traffic to ArcGIS Server).

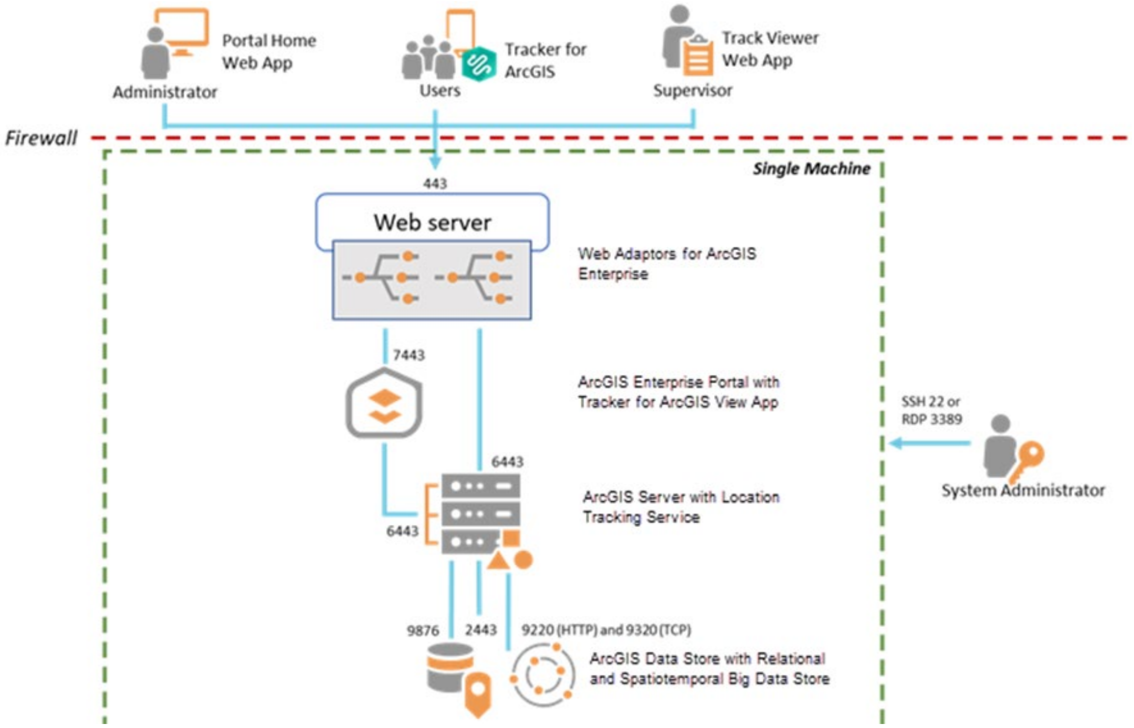

Portal Home Web App
Administrator
Tracker for ArcGIS
Users
Track Viewer Web App
Supervisor
Firewall
Single Machine
443
Web server
Web Adaptors for ArcGIS Enterprise
7443
ArcGIS Enterprise Portal with Tracker for ArcGIS View App
6443
6443
ArcGIS Server with Location Tracking Service
SSH 22 or RDP 3389
System Administrator
9876
2443
9220 (HTTP) and 9320 (TCP)
ArcGIS Data Store with Relational and Spatiotemporal Big Data Store

Figure 6—ArcGIS Enterprise Single-Machine Deployment with Location Sharing

Advantages

- Simplest on-premises deployment, since it only requires one machine
- Least expensive on-premises or cloud deployment pattern
- Reduced backend inter-server clear-text transport concerns due to consolidation to one system
- Customer in full control of the data life cycle

Disadvantages

- Typically, inadequate for meeting privacy regulatory requirements
- Availability and scalability limitations—Single point of failure
- Performance limitations – Recommend Spatiotemporal Big Data Store installed on separate ArcGIS Datastore host
- Customer responsible for ensuring that data is encrypted at rest

Recommendations

This deployment is ideal for proof-of-concept use cases typically utilizing anonymized data instead of PII. If PII is going to be used in a proof-of-concept validation process, then Esri strongly recommends implementing additional security and privacy measures to meet the privacy needs of the organization/relevant regulations. At a minimum, encryption of data at rest should be implemented by the customer, using third-party software, and periodic scans performed for alignment with security best practices with the ArcGIS Enterprise security validation tools.

3.3.4 ArcGIS Enterprise—Multimachine

In this configuration pattern, the enterprise stack (Portal for ArcGIS, ArcGIS Server, and ArcGIS Data Store) is distributed across multiple machines. This deployment utilizes one machine running Portal for ArcGIS, one machine running ArcGIS Server, and one machine running ArcGIS Data Store, as seen in figure 11 below.

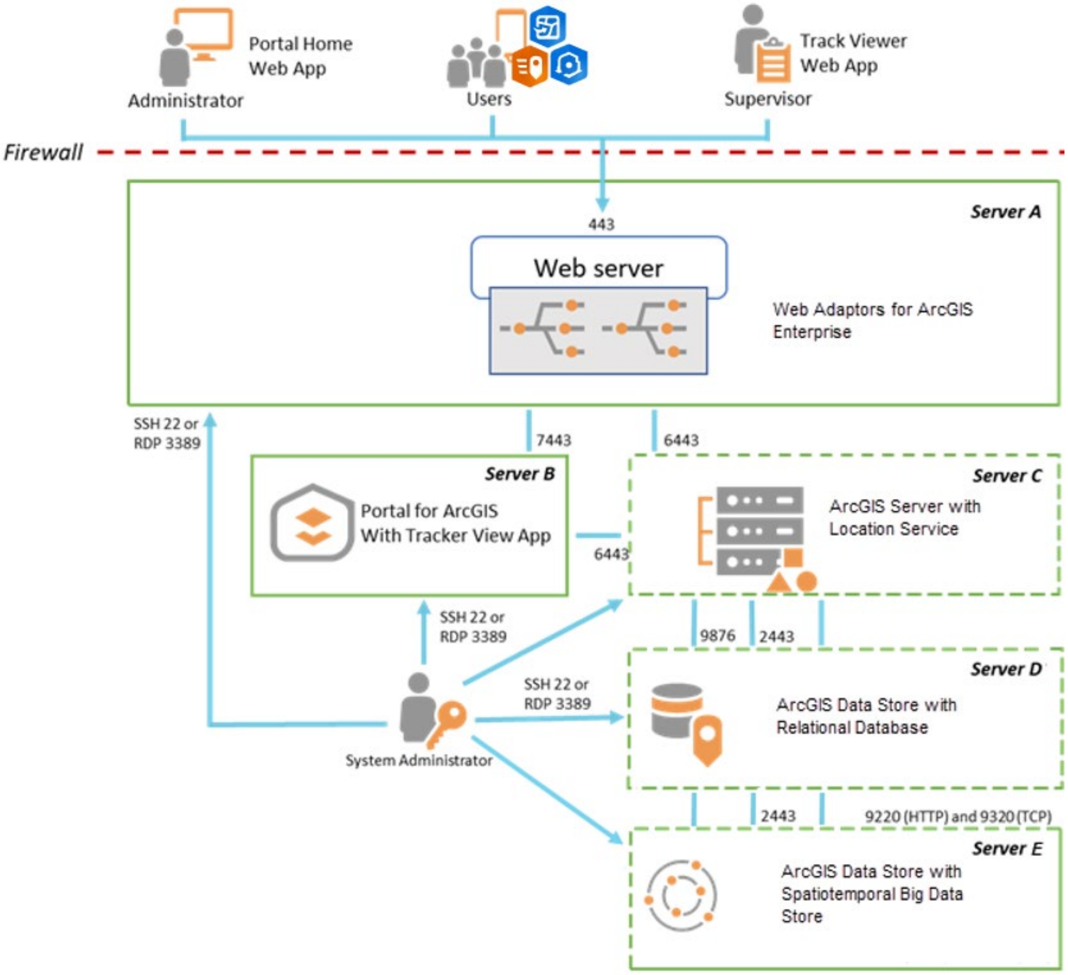


Figure 7—ArcGIS Enterprise Multimachine Deployment with Location Sharing

Advantages

- Typically, better performance than single-machine deployment
- Ideal for small-to-large enterprises with heavy workloads
- Customer in full control of the data life cycle

Disadvantages

- Increased administrative overhead/complexity with multiple machines to maintain
- Increased total cost of ownership, since there are multiple machines in the deployment
- No redundancy if a system fails
- Backend transport between ArcGIS Server and ArcGIS Data Store not encrypted

Recommendations

Ideal for medium-to-large organizations where scalability and performance are critical, but availability and the privacy of their information is not critical. Organization should ensure that backend communication between systems is encrypted, such as with IPSec at operating system level; also, the customer will need to utilize third-party offerings to encrypt data at rest. Though backend security and DMZ layers are not represented within this deployment, some additional security infrastructure is necessary to meet even minimal privacy assurance requirements.

3.3.5 ArcGIS Enterprise—High Availability

In this configuration pattern, multiple ArcGIS Enterprise components are working together with the organization's underlying security infrastructure components to maximize privacy assurance and uninterrupted service. The ArcGIS Enterprise components stack is in a paired formation with two Portal for ArcGIS machines, two ArcGIS Server machines, and two ArcGIS Data Store machines.

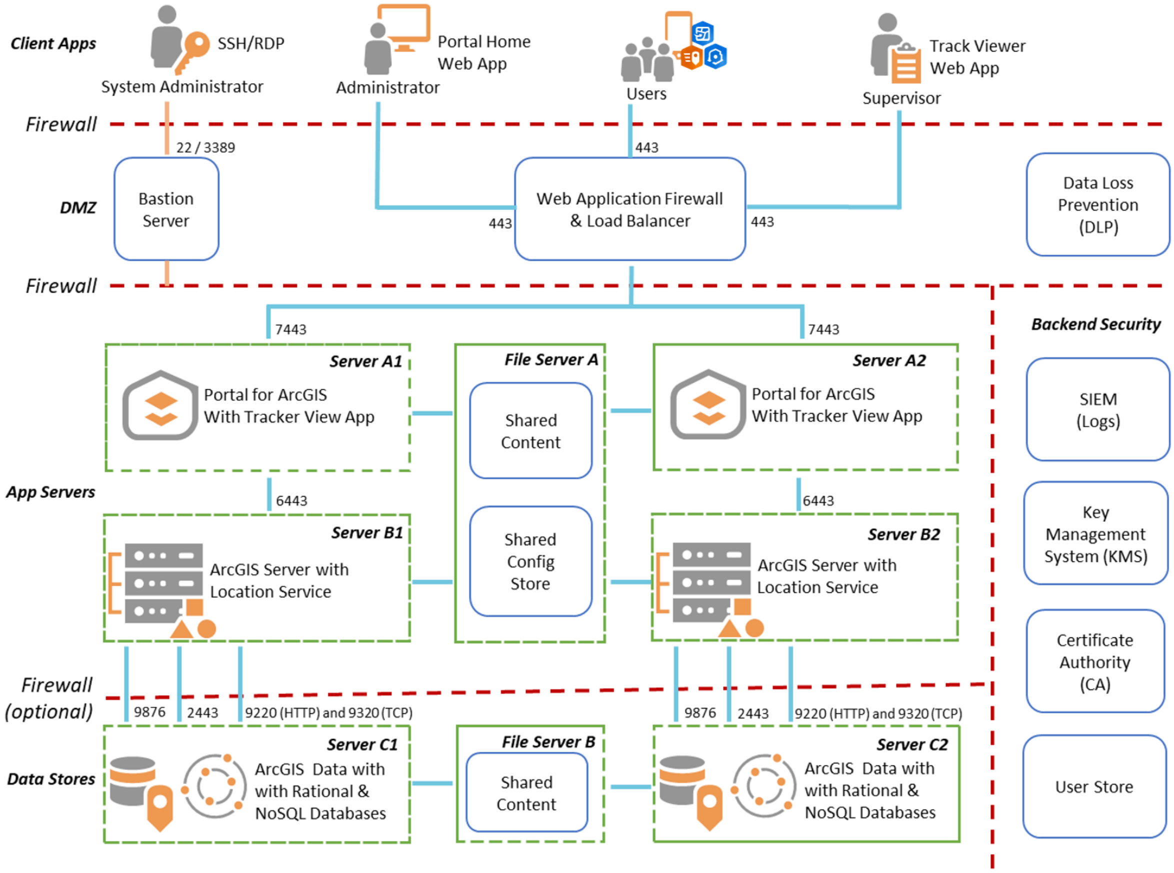


Figure 8—ArcGIS Enterprise High Availability Deployment with Location Sharing

Notes

- *Portal for ArcGIS*—Machines (Server A1 and A2 in figure 12) store content in the same directory (Shared Content), which must be placed on a highly available file server, such as network-attached storage (NAS). If the primary server-portal 1 becomes unavailable, then the standby server-portal 2 takes over. Portal for ArcGIS HA does not support an active-active configuration.

- *ArcGIS Server*—Machines (Server B1 and B2) which are the hosting servers, share server directories and a configuration store (Shared Config Store and Directories), which must be placed on a similar highly available file server.

- *ArcGIS Data Store*—Machines (Server C1 and C2) are registered to the hosting server. ArcGIS Data Store has a built-in failover mechanism whereby the standby relational data store becomes the primary data store machine if the primary machine fails.

Advantages

- Provides high resilience to failure at all levels of the deployment
- Typically provides better performance than single-system deployment
- Supports large organization mission-critical use cases
- Customer has full control of the data life cycle
- Utilizing centralized file systems for both configuration and directory information minimizes PII stored on individual servers

Disadvantages

- Highest total cost of ownership compared to all deployment patterns above
- Requires high level of administrative expertise to maintain
- A maximum of 2 Portal machines can be configured per site.
- Applying third-party components to encrypt data at rest and for transport between servers

Recommendations

This deployment pattern is recommended for medium to large organizations where the availability and redundancy requirements are high. Typically, this is driven by specific service-level agreement (SLA) requirements such as four 9's and higher, or a very low Recovery Time Objective (RTO). An RTO is the maximum tolerable length of time that a system, network, or application can be down after a failure or disaster occurs.

3.4 Location Sharing with ArcGIS Field Maps and ArcGIS QuickCapture

Location sharing consists of three sets of components, shown in figure 13, that were introduced in section 2:

- End-user apps for enabling location sharing and viewing
- Professional apps and tools for viewing/sharing tracks and creating feature service views
- Location services backend infrastructure

This section provides more details about these components and discusses user patterns specific to Location Sharing.

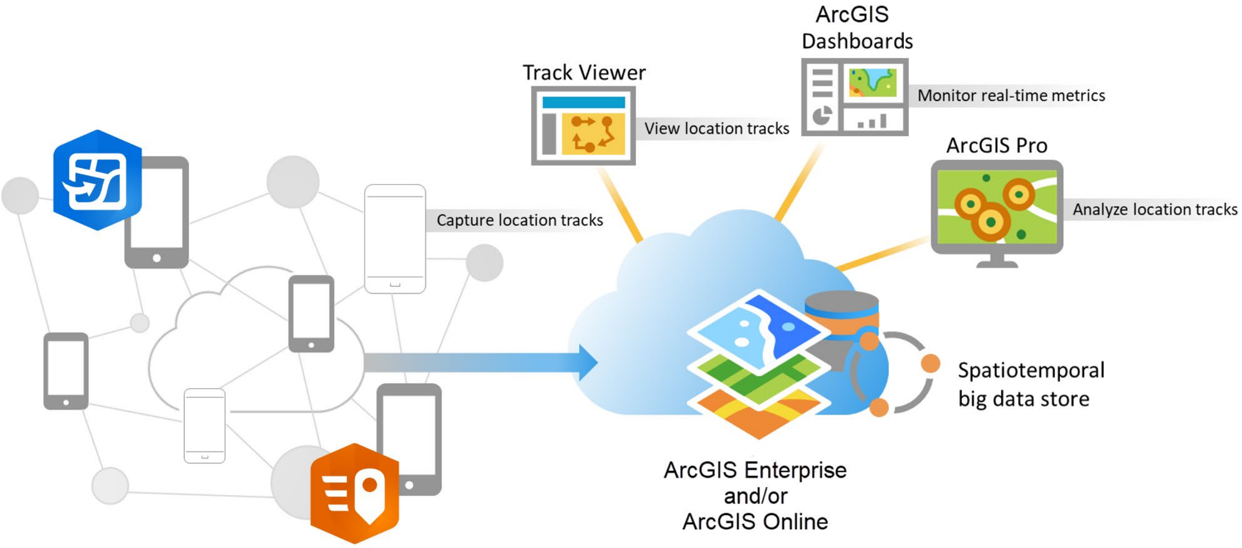


Figure 9—Location Sharing Deployment Components

End-User Apps Facilitating Location Sharing and Viewing

- To sign into the apps and leverage location sharing, users need to be assigned a Mobile Worker User Type or a User Type with the Location Sharing User Type extension by their administrator. The Location Sharing User Type Extension license is available for use with any user type—including Viewers.
- The apps support offline use.
- The apps are optimized for low battery consumption.

Professional Apps and Tools for Viewing Tracks and Creating Feature Service Views

- Track Viewer web app allows authorized users to view location tracks.
  - Administrators can create track views that include the list of mobile users being tracked and users that can view their tracks.
  - Users with the “View location tracks” privilege are granted access to track views and can visualize and interrogate tracks using Track Viewer or add the view to other web and field applications.

- ArcGIS API for Python has a sharing module that lets users automate common location sharing administrative tasks.
- ArcGIS Pro provides advanced analysis tools to let users review workers' location tracks and perform more complex tasks such as validating inspection reports, confirming assignment coverage, and planning for the next day.

Location Services Backend Infrastructure

- ArcGIS Enterprise 10.7 or later includes a spatiotemporal big data store[7] for storing and serving location tracks.
    - An ArcGIS Enterprise Standard license or higher is needed to deploy location sharing; all the GIS Server functionality and the spatiotemporal big data store is included in that license.
- A variety of server roles and extensions can be added to further supplement your location sharing services with ArcGIS Enterprise:
    - ArcGIS GeoEvent Server—GeoEvent™ Server is not required for Location Sharing; however, it can be used to complement location sharing, such as notifying when a worker has arrived or has left a work location.
    - ArcGIS GeoAnalytics Server—Analytical functions generate new datasets from location sharing services. Functions such as aggregation can result in the new dataset being less sensitive, but other functions could have the opposite effect. Planning for appropriate management of the source and analytical output datasets is important to a rigorous privacy program. GeoAnalytics Server can be used to provide meaningful insights by using the following tools:
        - **Reconstruct Tracks—**This is useful for creating lines from track points to show direction and to generate new line work (which could be turned into a transportation network).
        - **Aggregate Points—**Can be used to analyze coverage over an area, such as the area searched during a rescue operation or the percentage of a utility corridor covered when performing an inspection. Aggregation offers a great way to minimize exposure of PII, as discussed further in section 3.6.2.
        - **Detect Incidents—**When studying movement, the Detect Incidents tool can identify rapid changes in speed so long as speed is an attribute in your data.
        - **Find Point Clusters—**By using a density-based clustering method, you can identify frequently visited locations based on the movement of your workforce.

[7] Find more information about the spatiotemporal big data store.

3.4.1 Location Sharing User Patterns

Location Sharing has three primary user patterns with associated roles and permissions as described below:

- Administrator
    - Role: Administrator
    - Permissions: All
    - URL: https://MyOrg.MyDomain.com
- Supervisor
    - Role: Custom role
    - Permissions: View location tracks
    - https://MyOrg.MyDomain.com/portal/apps/trackviewer
- User
    - Role: Viewer
    - Permissions: Viewer
    - URL: https://MyOrg.MyDomain.com/portal

Administrator

Before enabling the location sharing service in ArcGIS Enterprise, administrators should ensure that their deployment plans are in alignment with their organizational privacy policies and practices. Administrators should be transparent with their organization's employees about location sharing and tracking services and how users can control what information is tracked.

Administrators have full control of the Location Sharing deployment. The location sharing service is based on a single hosted feature layer, which is controlled by the administrator who enabled the service.

As part of daily operations, administrators can perform the following:

- Create track views:
    - Track views contain the last known location and history of previous mobile user locations.
    - Multiple track views can be created:
        - Each track view establishes a new group with an associated track name.
        - Feature layer views are shared within the group.
- Grant access to track views to anyone who needs access.
- View how many members can view tracks.
- Configure retention period from a default of 30 days to any desired time frame.
- Pause the location sharing service (all administrators).
- Start and stop the service (only the administrator who enabled the location sharing service has this ability).
- Change ownership of the location sharing hosted feature service:
    - If there is a need to have another administrator take ownership of the location sharing service, then the current administrator must change ownership of the location sharing hosted feature layer to the desired administrator. The previous administrator will lose the ability to disable the location sharing service once this is done.
- Delete track views.
- Disable and remove the location sharing capability.

Supervisor

Supervisors are typically users that don't have administrative responsibilities but can view their respective team members' tracks, as shown in figure 14. They can be granted permissions to view these tracks by the user who created the tracks or the organization's administrator.

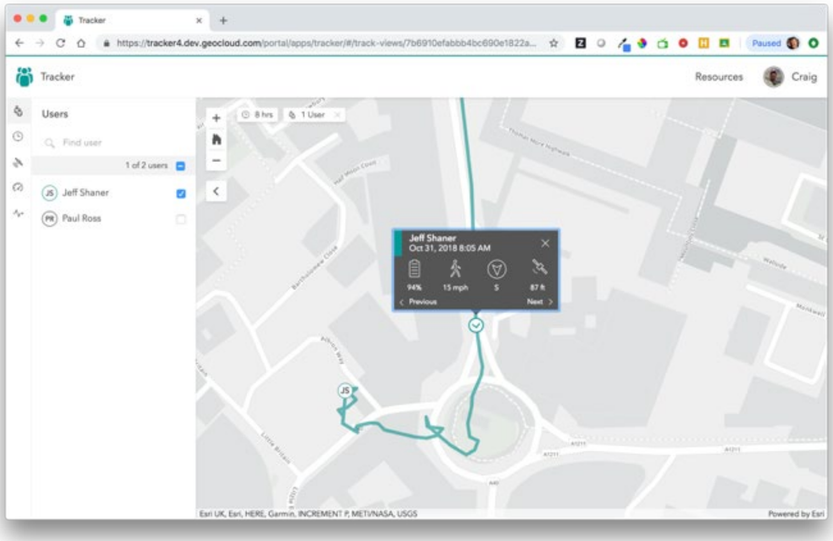


Figure 14—Supervisor Track View

Note: Anyone granted the View location tracks content privilege can view locations of mobile users within a track view. This is an ideal role for a supervisor's assignment. To ensure transparency and privacy for all users, instances where the administrator grants track view privileges to a user who is not the owner of the tracks should be communicated to the tracks owner before granting access.

Supervisors can open the Track Viewer application to display user tracks, which includes

- Default display of the last eight hours.
- The ability to click on tracks to view details, as shown in figure 14 above.
- Track data filtering by time span or accuracy.
- Highlighted views of an individual user's specific tracks by speed or even their activity.

Note that track views can be added to other web apps for supervisors to display tracks as well.

User

Users are members of the organization who have the privilege to view content shared with their organization, but no administrative abilities. Note: User is also a role in both ArcGIS Enterprise and ArcGIS Online. For information on privileges and user types, see the User types, roles, and privileges help topic.

As part of daily operations, users can perform the following activities:

- **Enable mobile device location sharing —**Mobile users are in complete control of when their location is being recorded and shared and can turn on/off tracking from their mobile devices at any time.
- **View tracks—**For privacy and security concerns, users can only see the tracks they created, since privileges are set according to ownership-based access control (OBAC). Think of ownership-based access control as discretionary access control (DAC), where the administrator of the track view determines the permission other users have to view their location. Users must have the View location tracks content privilege to see the tracks of other users.

3.5 ArcGIS Indoors

Indoors is built on Esri's desktop, enterprise, web, and mobile technologies. This section provides more details a typical deployment of ArcGIS Indoors.

End-User Apps Facilitating Location Sharing and Viewing

- ArcGIS Indoors mobile app—For Android and iOS—View indoor maps; get directions; and share accurate, real-time locations inside and outside buildings.
    - Users can view indoor maps, search for and save points of interest, reserve workspaces and meeting rooms, and get landmark-based directions—all by using a mobile device. The apps also support interfacing with indoor positioning system (such as ArcGIS IPS or Apple's IPS), allowing users to see and share their accurate, real-time locations when inside a building.
- ArcGIS Indoors web app—Look up building resources via a browser or kiosk for visitors or employees.
    - Allows users to find a location or resource within a building or site
    - Can be configured to run in two modes: a browser mode for users in the organization that need to access indoor information from their computer or device, and a kiosk mode for visitors to use from a touch screen device in a reception area
    - Allows anonymous users to see non-sensitive information about your buildings (Anonymous access to user location or building footprint information should undergo a high-risk privacy and security review.)

Professional Apps and Tools for Creating and Managing Indoor Data

- ArcGIS Pro—Ability to create indoor GIS datasets, then author and share floor aware maps via the Indoors Pro extension, then to publish for use with Indoors and ArcGIS.
    - Included with the Indoors Maps or Indoors Spaces license levels is the Indoors user types, which provide an identity in ArcGIS Enterprise or Online.
    - Before using Indoors, you need to create indoor data in ArcGIS Pro with the Indoors extension, then publish the data for use.
- ArcGIS Indoors Information Model—A model for the indoor GIS datasets, feature classes, tables, and database configurations
    - Configure the web maps and mobile map packages used with Indoors apps.
    - More information is available in the ArcGIS Indoors Information Model help topic.

Location Services Backend Infrastructure

- Specialized ArcGIS Enterprise deployment is used by Indoors for database support, data sharing, publication, and analysis.
    - Indoors relies on ArcGIS Enterprise or ArcGIS Online for database support, data sharing and publication, and analysis.
- Spatiotemporal big data store is used to store real-time location sharing data.
    - Can store and manage very large datasets and is able to store and retrieve data very quickly
    - Allows Indoors to ingest and record data at the very high rates needed to support large amounts of incoming real-time data

- ArcGIS GeoEvent Server can be used to create indoor geofences and trigger actions and alerts when certain conditions are met.
    - GeoEvent Server subsequently passes real-time information into other apps, including web maps and dashboards.

If datasets are not strictly managed, location data with PII may end up on a variety of systems across the enterprise. Limiting the number of systems that download location PII datasets locally on each device and ensuring that end-user devices automatically clear their caches on a regular basis are crucial for honoring PII data minimization principles. Assurance that all communications in transit and data at rest are encrypted is also a vital component of user privacy.

3.6 Privacy Security Considerations

This section provides key architectural guidelines relative to the sensitive nature of handling PII with a location sharing service, including the following:

- Limiting service endpoint access
- Limiting data collection
- Limiting user information exposure
- ArcGIS Online privacy considerations
- ArcGIS Enterprise privacy considerations

If you are an administrator of ArcGIS products, as you read through the below considerations, please refer to section 8.1 ArcGIS System Security and Privacy Best Practice Configuration Settings for guidance concerning specific settings of both ArcGIS Enterprise and ArcGIS Online.

Please refer to the *ArcGIS Secure Mobile Implementations Patterns* technical paper for an overview of recommendations for securing the infrastructure supporting your mobile applications.

3.6.1 Limiting Service Endpoint Access

One of the more secure approaches for limiting access to your location sharing endpoints is to utilize a virtual private network (VPN) solution. Unfortunately, VPN solutions typically require more user interaction to manage, slow performance of the application, and take up significantly more battery power if location sharing data is to be enabled on devices throughout the day. Some organizations utilize security gateways or mobile device management offerings that operate in a more transparent manner. If these are not an option, you can consider establishing geo-restrictions for IP addresses attempting to access your operations from locations around the globe. Geo-restrictions for IP addresses can also be a useful tool for organizations not prepared to meet privacy obligations for various regions around the world, such as the European Union for GDPR or the State of California for CCPA. A number of large newspaper companies in the United Stated blocked access to their websites to EU citizens to delay their GDPR obligations as their systems were modernized for new privacy obligations.

- **VPN-Corporate—**Access to your ArcGIS Enterprise deployment can be made using the corporate VPN. However, this option can be costly to implement if it is not already in place. This option is ideal whenever you access your enterprise solution via any publicly provided internet connection such as airport Wi-Fi.
- **Mobile device management (MDM)—**Access to the location sharing service can be restricted through an MDM deployment by the organization. This option is ideal for organizations with a need for complete device and application control.

- **Geo-restriction—**Restriction can be done at the infrastructure level, such as a cloud provider service. This restriction is commonly based on country, region, or state. This solution is not foolproof, as IP addresses can be spoofed; however, it will significantly reduce hits against your internal systems.
- **Certificate pinning—**This is ideal when you want to be sure that all remote users identify themselves before consuming resources from your organization. This provides a layer of defense against man-in-the-middle (MITM) attacks, where a forged certificate is used.

3.6.2 Limiting Data Collection

Minimizing how much PII you need to collect can significantly reduce your privacy-related liabilities. Options to limit data collection include the following:

- **Disabling location sharing—Server side—**Location sharing services can be disabled from the server as an avenue to limit data collection during a specified schedule or for special events. Disabling location sharing is managed by the ArcGIS administrator.
- **Geofencing—**This option is ideal when location sharing is paired with the geofencing capabilities of ArcGIS GeoEvent Server and in ArcGIS Field Maps. This option is also useful for monitoring use cases to draw zones or predefined borders around a school area or any classified secure areas. If these zones are crossed, then a warning or alert can be triggered immediately.
- **Scheduling—Client side—**This option is available in some mobile apps. Mobile users can choose how long location sharing will remain enabled. When this duration expires, location sharing stops automatically
- **Aggregation—**Raw PII dataset streams frequently don't need to be distributed outward. Instead, the data can be aggregated to a level where it is no longer considered PII and then shared. A service could potentially create an aggregate dataset each evening and the raw PII dataset deleted. Since GPS data from location sharing is typically considered personal information by default, if you want to avoid handling your location data under the constraints of PII, avoid handling/storing fine-grained location information as defined under your regulatory obligations. Truncating spatial datasets to 1 (city level) or 2 (village level) decimal places can help meet obligations to avoid handling the data as PII.
- **Deidentification—**If you don't have a need to keep full, detailed latitude-longitude data for users, consider a deidentification approach, such as truncating the latitude-longitude information to a certain level of digits or replacing latitude-longitude information with the name of the city.

3.6.3 Limiting User Information Exposure

Users today frequently utilize passwords between sites, and the more sites where the same password is stored by separate service providers, the more likely that information will be part of a breach. Utilizing enterprise logins via SAML against your organization's centralized identity provider means one more piece of PII you don't have to store in your location sharing systems (password hash). An overview of authentication options for ArcGIS products follows:

- **Built-in security—**This is the default built-in security model where user and role information is stored within ArcGIS Online. Mobile devices connect to ArcGIS Online and provide credentials. Some considerations with built-in accounts are when a user separates from the organization, you must remember to deactivate the account in the ArcGIS solution since it is not tied into the customer's centralized account management systems. Esri recommends to always enforce MFA on all administrator accounts.
- **Enterprise logins with SAML—**In this option, the ArcGIS Online organization is registered with a third-party IdP to verify credentials. Users requesting to login are directed to the IdP. They log in

to the IdP, which verifies their credentials and provides an authentication token to allow them to log in to ArcGIS Online. Esri strongly recommends this option for better security.

- **Multifactor authentication—**This option is a best practice that adds an increasingly important layer of protection on top of your user name and password. Esri recommends MFA on all administrative accounts (at a minimum) for ArcGIS Enterprise or ArcGIS Online.
- **Social logins—**Authentication via a social network, like Google or Facebook, is supported. Typically, the users associated with the accounts have not been vetted as strongly as business accounts, so you typically have less assurance of who you are dealing with. Also, ArcGIS Online administrators cannot enforce password resets of social login accounts, and none of the ArcGIS Online password policy requirements apply to the social login accounts. These social login deficiencies can significantly degrade the security and privacy posture of your operations. **Note:** Even though this option is available, Esri strongly recommends using this with caution, and where possible, organizations should avoid using this option.

3.6.4 ArcGIS Online Privacy Considerations

ArcGIS Online maintains a FedRAMP Tailored Low authorization, which ensures that rigorous security mechanisms and procedures are in place. Customers with datasets incorporating PII frequently make use of ArcGIS Online services as a central part of their geospatial platform using hybrid deployments.

User Profiles

Organizations with rigorous privacy concerns typically disable user profiles from being populated by users. The ArcGIS Online administrator may enable this feature by deselecting the option to allow members to edit biographical information and who can see their profile. If your organization currently has profile information, you can limit PII through your organization's governance processes; administrators or users may remove profile details, or individual users may disable their profiles. Organizations that leverage SAML can elect to map a unique user attribute that does not contain PII to the mandatory ArcGIS Online named attribute. Customers that do not wish to provide unauthenticated access to their ArcGIS Online organization should disable anonymous access.

Publishing

The publisher role is a powerful role. Provisioning rights to administer or publish to an ArcGIS Online organization is a decision that should not be taken lightly. Care and oversight should be used when making decisions as to the nature of the data that is published. In general, ArcGIS Online organizations are not particularly prone to breach by an external entity. Instead, it is considerably more likely that an individual inside the organization accidentally publishes datasets containing private information due to lack of familiarity with the application capabilities or with privacy best practices. Developing training, maintaining a culture of accountability, and establishing content review procedures are critical activities to mitigate this risk. Establishing these practices prior to assigning a user publisher privileges that allow them to publish is extremely important to help prevent inadvertent disclosure of private information.

Validate Alignment with Best Practices

To ensure that your organization is making the best use of the security capabilities available within ArcGIS Online, Esri has released a security best practices validation tool for ArcGIS Online. The ArcGIS Online Security & Privacy Advisor can be launched directly from the ArcGIS Trust Center at

Trust.ArcGIS.com. Use the ArcGIS Online Security & Privacy Advisor to validate that your current ArcGIS Online policies and settings are in alignment with security and privacy best practices.

Location Sharing includes 30 days of location track storage within ArcGIS Online. Tracks can be exported most effectively as CSV files and archived manually by customers.

Current Limitation Using ArcGIS Online

The ArcGIS Online back-end database does not currently support advanced analytics. This means some operations will not be available for advanced reporting in applications like ArcGIS Dashboard or when using the analysis tools. There are plans to bring these features to the location sharing feature service in the future.

3.6.5 ArcGIS Enterprise Privacy Considerations

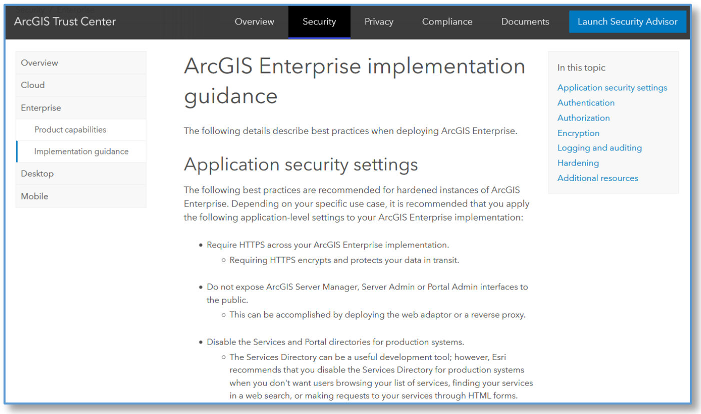
Esri performs security hardening steps against ArcGIS Online to maintain its FedRAMP authorizations. Customers should ensure that appropriate security hardening is performed against their ArcGIS Enterprise deployment.

Frequently, customers utilize the Center for Internet Security (CIS) Benchmarks or Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS) to harden their infrastructure. Note that Esri has an ArcGIS Server STIG available for helping harden a key component of your ArcGIS Enterprise deployment. There are also basic security validation Python scripts (serverScan.py and portalScan.py) available for ArcGIS Enterprise that should be scheduled to periodically execute to check for configuration drift. These tools may be called via a cron job or the Windows Task Scheduler.

To minimize exposure of user profile (personal) data, administrators can disable the ArcGIS Portal Directory. Disabling the ArcGIS Portal directory prevents users from browsing your lists of items, finding your services in a web search, or making requests to your portal through HTML forms.

Don't overlook the value of your endpoint logs generated by appliances in front of your ArcGIS Enterprise services. Periodically review the web server log files generated on the server where your Web Adaptor is deployed, or by your Enterprise load balancer or other gateways. These systems should be configured to log each request to ensure that all activity against your endpoints is appropriately monitored, allowing your organization to more effectively identify potential data loss issues.

Additional guidance for hardening your ArcGIS Enterprise deployment may be found within the ArcGIS Trust Center (see figure 16).



ArcGIS Enterprise implementation guidance

The following details describe best practices when deploying ArcGIS Enterprise.

Application security settings

The following best practices are recommended for hardened instances of ArcGIS Enterprise. Depending on your specific use case, it is recommended that you apply the following application-level settings to your ArcGIS Enterprise implementation:

- Require HTTPS across your ArcGIS Enterprise implementation.
  - Requiring HTTPS encrypts and protects your data in transit.
- Do not expose ArcGIS Server Manager, Server Admin or Portal Admin interfaces to the public.
  - This can be accomplished by deploying the web adaptor or a reverse proxy.
- Disable the Services and Portal directories for production systems.
  - The Services Directory can be a useful development tool; however, Esri recommends that you disable the Services Directory for production systems when you don't want users browsing your list of services, finding your services in a web search, or making requests to your services through HTML forms.

Figure 16—ArcGIS Trust Center Security Guidance

4 Corporate Privacy Controls

Your organization is responsible for ensuring that privacy policies and procedures are enforced across your operations. This section provides a summary of items that should be addressed by your system administrators and supervisors who manage the enterprise infrastructure supporting the location sharing services.

4.1 Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is a series of questions that evaluate the processes through which personally identifiable information is collected or created, stored, used, shared, archived, and destroyed by an electronic information system or online application.

Esri has begun conducting PIA's against new products and services or when significant changes to existing products and services make sure the following is addressed:

- Conformance with applicable privacy regulations, legislations, and policy requirements
- Assessment of the risks and evaluation of alternative mitigation measures

Esri's privacy assessment is composed of the following:

- Thorough understanding of information to be collected
- Why information is being collected or its intended use
- Review of all components required for the service to function
- Threat modeling exercise to identify threats to privacy as well as mitigation measures

Customers are encouraged to conduct a PIA to ensure that privacy needs for their organization are being met. A privacy threshold analysis should be completed first to identify the type of information that will be exchanged, with whom it will be exchanged, and whether there are any associated privacy concerns. If the threshold is met for private information, then a PIA should be conducted that includes answering how information is collected, stored, used, and disposed of. Many customers are required by law to complete a PIA based on the regulations that govern the industry or region they are operating in. If a customer requires assistance with conducting a PIA, they should reach out to Esri for assistance at SoftwareSecurity@esri.com.

4.2 Privacy by Design

Esri ensures data privacy by design (PbD) by incorporating security and privacy practices throughout the secure product development life cycle. Technical controls are implemented, allowing end users to manage how data can be processed and shared in a secure manner.

Encryption at Rest

All customer data in ArcGIS Online is encrypted by default to provide security and privacy assurance to our customers. For on-premises deployments, the ArcGIS administrator should coordinate with the organization's security team to make sure encryption at rest is implemented. For mobile use cases, encryption can be enforced by leveraging an MDM deployment.

Encryption in Transit

All communications between the client and ArcGIS Online location sharing services are secured using HTTPS via TLS 1.2 only to provide privacy of customer datasets when in transit. For on-premises deployments, the ArcGIS administrator has full control over the security of the configuration and can make the desired changes as needed including enabling HTTP Strict Transport Security (HSTS).

If you are new to HSTS, it is a web security policy mechanism that helps protect websites against protocol downgrade attacks and cookie hijacking. **Note:** The default configuration setting for ArcGIS Enterprise is HTTPS with TLS 1.2. HSTS enforcement across all ArcGIS Online organizations was implemented in 2020. Organizations can enforce encryption in transit for mobile use cases by leveraging an MDM deployment.

Data Classification

Customers have full ownership of their data stored by the location sharing service and therefore data classification is a customer's responsibility. ArcGIS Online has a FedRAMP Tailored Low Authorization to Operate (ATO), and data stored in the solution should be categorized accordingly. The risk categorization for an ArcGIS Enterprise deployment is determined by the organization's security and privacy needs.

User Application Activity Analytics

Collecting user activity analytics, which may contain significant amounts of PII, is commonly performed by both customers and software vendors today.

ArcGIS Online collects non-PII usage data via the Esri User Experience Improvement (EUEI) program by default for most organizations. The program is optional and anonymous; none of the information collected is used to identify or contact members of an organization. The organization administrator can disable the EUEI service at any time. The EUEI is disabled by default for ArcGIS Online European Union customers—this is in alignment with an opt-in approach, as required under GDPR. Further information about the EUEI program and the type of information collected can be found at support.esri.com/en/technical-article/000016235.

ArcGIS Enterprise does *not* have an option to collect EUEI information. Be aware that as new regulations such as CCPA take effect in 2020, if you are using third-party analytics tools against your ArcGIS deployment, you should look carefully at the vendor's terms. If the analytics company owns the analytics output, this could be considered a sale under the new California regulation (you are "selling" the analytics data to the provider to obtain its service), which has significant reporting/communication consequences you will need to be prepared to honor.

Security Mechanisms

ArcGIS Enterprise includes a number of robust security mechanisms to protect access to personal data stored within the system. ArcGIS supports both relational and NoSQL databases. User data other than location sharing services data is stored in the relational database, and location sharing data is stored in a NoSQL database. Worth noting is that the Java Database Connectivity (JDBC) from hosting server to ArcGIS Data Store is not encrypted. So Esri recommends encrypting communication between machines in your deployment, for example, enabling Internet Protocol security (IPSec) between clients—server, client-client; this way, all communication between machines in the deployment is over a secure channel. Also, for security and privacy of your data, Esri strongly recommends encryption at rest for all machines in the deployment.

4.3 Governance

Security policies spanning Esri are set at the corporate level under the guidance of the Chief Information Security Officer (CISO). Also, at the corporate level, the Legal and Human Resources Departments ensure alignment with evolving privacy needs, including vetting employees before onboarding, and pushing for advancement of business continuity efforts. Corporate security controls are inherited across Esri, while functional areas (such as engineering and operations) are responsible for specific security control families.

The security and privacy of Esri products and services are overseen by the Chief Information Security Officer CISO—Products, who leads Esri's Software Security and Privacy team. This team is embedded within product operations and engineering, providing both security/privacy guidance and validation while fostering champions across the broad spectrum of product teams to help further ensure security/privacy across Esri products.

Under GDPR, Esri has appointed a Data Protection Officer (DPO) and an EU Representative. Our DPO works to ensure that Esri processes the personal data of its staff, customers, providers or any other individuals in compliance with the applicable data protection rules. Esri also has a Chief Privacy Officer (CPO) to ensure that privacy is addressed holistically across Esri, as well as the CISO for Products, who oversees privacy of products and FedRAMP authorized services such as ArcGIS Online. To operate as a privacy resource, individuals must maintain an industry-standard privacy certification, such as from the International Association of Privacy Professionals (IAPP).

For additional information regarding Esri software security, privacy, and compliance, check out the ArcGIS Trust Center. For customers utilizing ArcGIS Online for location sharing services, please refer to the Cloud Security Alliance (CSA), Consensus Assessment Initiative Questionnaire (CAIQ) for more extensive, solution-specific governance information.

Applicable Laws and Regulations

Privacy legislations may vary from one state to another and from country to country. Esri is committed to compliance with regulations and laws, such as GDPR, by providing privacy protection to all our customers. Esri has a Data Processing Addendum (DPA) that sets the conditions related to privacy, confidentiality, and security of personal data associated with online services and maintenance that we provide to customers under a master agreement, customer's current license agreement with Esri, or the then current click-through agreement. The DPA contains data transfer frameworks, ensuring that our customers can lawfully transfer personal data to ArcGIS Online outside the European Economic Area.

4.4 Data Retention

Data retention is the continued storage of organization or personal data for a defined period as stipulated by the organization's retention policies or regulations that the organization conforms to. Privacy officers frequently focus on understanding the privacy risk involved with location sharing services, including what information types are collected, why, when, and the associated retention periods.

One of the biggest challenges organizations face today is information life cycle management. Organizations should avoid being caught in the state of *collect* rather than the *use* state where a huge amount of information is collected without a clear plan of what to do with it. Doing this violates a fundamental privacy principle: Only collect information that you need to fulfill the purpose for which it is collected.

Esri location sharing services provide an option to configure a retention period. ArcGIS administrators can configure a retention period ranging from 30-days to one year to align with the respective regulatory requirements for ArcGIS Enterprise deployments. ArcGIS Online default retention is 30 days. If a customer has a requirement for data retention that is beyond the default in ArcGIS Online, then tracks should be exported out of the solution in CSV format.

4.5 Breach Notification

ArcGIS Online
Esri is committed to protecting your personal information from attacks or data breaches. We have implemented appropriate security controls throughout our business systems. In the unlikely event of a data breach, we will provide notification within 72-hours of a confirmed breach of your data.

ArcGIS Enterprise
ArcGIS administrators should consult with their security and privacy team to determine the regulatory requirements that are set forth for their organization.

Customers should ensure that their breach notification processes address their applicable regional laws and industry requirements for various types of data incorporated into their deployment (PII, protected health information [PHI], etc.). To provide you with a starting point for identifying relevant laws if you are located within the United States, Perkins Coie, a security consulting company, keeps an updated chart of breach notification requirements across each of the 50 United States.

4.6 Auditing

Extensive logging is available within ArcGIS Enterprise and ArcGIS Online. Audit logs are only available to and accessible by ArcGIS administrators. Esri recommends setting the ArcGIS Enterprise log setting at the Fine level to capture the broadest number of security/privacy related events without overtaxing a system. Web server logs should also be enabled to track all web traffic to supplement the ArcGIS Enterprise logs. If you have a cloud-based deployment of ArcGIS Enterprise in Amazon Web Services, the following logs are frequently also useful: AWS CloudWatch, CloudTrail, Elastic Beanstalk (EB), and CloudFront logs.

ArcGIS Online provides customers with activity logs that can be exported as a CSV. These logs can be used to audit user activity against a specific resource. ArcGIS Online undergoes third-party assessments annually by certified third-party assessment organizations (3PAO), the results of which may be shared with your organization under a non-disclosure agreement (NDA).

4.7 Right to Be Forgotten

An increasing number of privacy regulations require that personal data must be erased immediately when the data is no longer needed for its original processing purpose, or the data subject has withdrawn consent and there is no other legal ground for processing. In the case of an erasure request, the data subject must be informed within one month about the measures taken or the reasons for refusal.

Exceptions to the right to be forgotten are worthwhile to note, as this requirement would otherwise severely hamper business transaction history requirements. Key exceptions include legal obligation, archiving purposes in the public interest, scientific or historical resource purposes, and business transaction requirements (such as financial obligations).

ArcGIS contains standard tools for deleting individual records and data tables within the system; combined with the search and identification tools, these can be used to remove personal data from your system. The Delete Features tool can be used to remove individual records from the ArcGIS system. The Delete Table and Delete Feature Class tools will enable you to remove datasets containing personal data.

Although the location sharing service doesn't advertise the delete capability in the feature service definition, administrators can delete tracks through ArcGIS REST API using the delete features operation. Go to the delete features REST endpoint for the tracks layer, where you can specify a WHERE clause or object IDs to identify and delete tracks. The URL of the delete features REST endpoint follows the format https://host.domain.com/webadaptor/rest/services/Hosted/location_tracking/FeatureServer/0/deleteFeatures (where host, domain, and webadaptor are replaced by the information about your server). These capabilities are not only critical for meeting forget me requests, but processes for utilizing them should also be formalized and implemented for when an employee leaves the company.

Restriction of Processing—With ArcGIS Online, records can be identified, exported, and deleted upon receiving a verified request to restrict processing. If the restriction is lifted later, the records can be reimported.

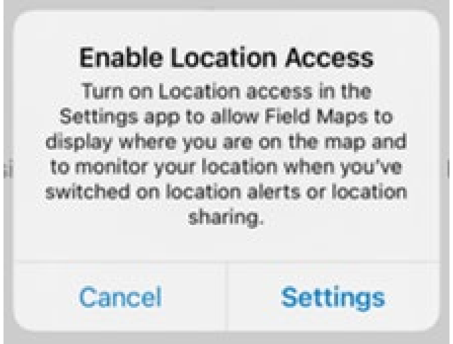
4.8 Consent

Consent is an agreement from a user for an organization to process their data in a certain fashion. Consent indicates a person gives permission for the use or disclosure of data. Consent may be affirmative or implied.

Affirmative/Explicit Consent
A requirement that an individual signifies their agreement with a data controller by some active communication between the parties; a user provides positive verifiable acknowledgment.

Implicit Consent
Implied consent arises where consent may reasonably be inferred from the action of the individual, such as an anonymous user browsing ArcGIS Online services is implied consent to ArcGIS Online privacy policy and terms of use. Worth noting is that most consent from users is implied consent, but regulations increasingly require explicit consent.

If ArcGIS is used to publish applications such as web apps that collect information from users, then it may be necessary to notify the users of an app that personal data is to be collected, and to link them to the relevant privacy policy. ArcGIS contains a range of mechanisms for notifying users of such policies:



Enable Location Access

Turn on Location access in the Settings app to allow Field Maps to display where you are on the map and to monitor your location when you've switched on location alerts or location sharing.

Figure 17—Enabling Location Sharing Services

- Within the ArcGIS Enterprise portal, administrators can customize the home page, as well as header and footer pages, which can include privacy statements or links.
- ArcGIS application templates enable you to configure a splash page for users before they access the application.
- Custom applications can include privacy notifications built using ArcGIS SDKs.
- Items stored in ArcGIS Enterprise and ArcGIS Online can include descriptions and usage limit statements that could contain any applicable privacy notices.

Esri helps you comply with data protection and privacy regulations with out-of-the-box support for indicating do not call, and email opt-out preferences. Esri also now includes an Individual Object for tracking your privacy preferences across our domains.

4.9 Data Portability

You can use ArcGIS Online or ArcGIS Enterprise to help honor your customers' requests to export their data. Data can be extracted via both GUI-driven as well as API-driven methods, including reports and report/dashboard APIs; REST APIs; and third-party extract, transform, and load (ETL) tools. Export formats include CSV, JSON, XML, and original source format. From the client device, all data collected is stored in a runtime database where no user interaction is possible. The Field Maps application uploads all collected tracks to the server when connectivity is available. Tracks that have been uploaded are removed from the device if they are more than 72 hours old to control the size of the database on the device.

4.10 Personal Data

An organization should have a privacy policy that outlines how information collected is going to be used and what choices you have as an end user. Esri provides details of what kind of information is collected when location services are enabled in either ArcGIS Enterprise or ArcGIS Online.

Your organization may need to consider establishing a process for handling Subject Access Requests (SAR's) concerning the location information stored. A SAR is when an individual exercises their right to find out what data is being held about them and how it is being used. Individuals may also ask for a copy of the data itself. When such requests are made, GDPR requires responding within one month (CCPA/CPRA requires 45 days) of receipt of the request or the customer may face legal proceedings and regulatory action.

Searching Data

While ArcGIS does not contain any tools designed specifically for identifying personal data, it does include several generic data search and analysis tools that can be used to search data and metadata for personal data. These can be combined with good data design and corporate standards around data dictionaries and metadata management.

- ArcGIS includes the ability to store metadata documents that reside with your data and describe the contents and data types.
- ArcGIS metadata documents are linked to the data and will move with the data as it is processed by ArcGIS.

- ArcGIS metadata documents can be searched for keywords and content describing personal data.
- ArcGIS includes database query tools that can be used to search within your GIS data for records that meet specific criteria.
- In addition to formal metadata descriptions, ArcGIS includes the ability to assign tags to categorize data. These can be used to tag items and layers that contain personal data and then included in future searches.

Correcting Data

One of the functions of a SAR is to assess if the user would like to correct some of the information stored about them. ArcGIS contains standard tools to allow users with the correct permissions to edit the content of data stored within the system. These tools can be used to correct or add to any personal data within ArcGIS.

- Data editing is controlled by user permissions and available only to authorized users.
- ArcGIS geometry editing tools can be used to edit location data.
- ArcGIS attribute editing tools can be used to edit attribute data stored in the GIS.
- Field Calculator tools can be used to make bulk changes to data.

5 User Privacy Controls

An important piece of ensuring appropriate privacy is providing users with clear guidance for what they can directly manage and control. This section should be of strong interest to users of location sharing products.

5.1 Right to Be Forgotten

As an end user, you have the right to erasure of personal information that an organization has collected from you. ArcGIS applications which use location sharing have a data retention control for data stored in the database on the device when the app is in use.

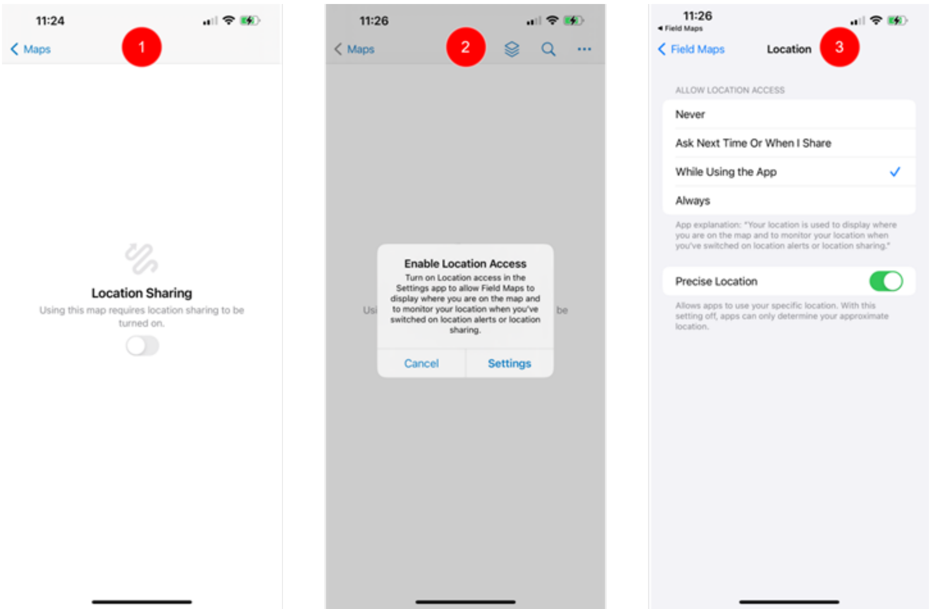
To ensure that your right to be forgotten is respected, when a mobile user signs out of ArcGIS Field Maps, ArcGIS QuickCapture, or ArcGIS Indoors, their information is cleared from the app and device, including any location tracks.

For controls on the server side, refer to the corporate-level privacy controls regarding the right to be forgotten.

5.2 Consent

Consent on the client side differs from the server side or corporation. When an end user installs ArcGIS applications which use location sharing from the respective store (Apple App Store, Google Play, or Microsoft Store), there are several prompts that the user must go through, such as signing in to the application and choosing to enable access to location. The following prompts are required for a user to be able to use ArcGIS applications which use location sharing on any device:

- Enable Location Services.
- Allow the application to access your location.
- Configure the settings to the desired level.



Using this map requires location sharing to be turned on.

Turn on Location access in the Settings app to allow Field Maps to display where you are on the map and to monitor your location when you've switched on location alerts or location sharing.

App explanation: "Your location is used to display where you are on the map and to monitor your location when you've switched on location alerts or location sharing."

Allows apps to use your specific location. With this setting off, apps can only determine your approximate location.

Figure 18—Enabling Location Services in ArcGIS Field Maps

Going through the steps above (as shown in figure 18) qualifies for an explicit consent on the end-user side. From this point, the mobile user has complete control of when they are recorded and when to share their location with others.

Note: The behavior documented above might differ if ArcGIS Field Maps or ArcGIS QuickCapture are pushed through an MDM deployment by the organization. Also, there is the ability to define a time duration after which ArcGIS Field Maps and ArcGIS QuickCapture automatically stops location sharing.

5.3 Data Portability

Data portability is the right to transfer personal or organizational data from one organization (controller) to anywhere of the subject's choice. Esri recognizes your rights to data portability, and as such Esri provides ways in which data can be exported out of the solution in a readily usable format to enable you to transfer information from one entity to another without hindrance. Other tools, such as the GeoAnalytics extract tool, can be used for data extraction from the solution. This is in alignment with GDPR Article 20. Also, customers have complete ownership of all their data collected and stored in the solution at any point in time.

5.4 Personal data

Under several privacy regulations, end users have the right to obtain information collected about them anytime (frequently called subject Access Requests, or SAR), and organizations should help foster this level of transparency. The process for a data subject to request information about them from their organization is not the same across all industries. Hence, Esri recommends that you review your organization's privacy policies regarding their preferred SAR submission method. That stated, these are some of the details you should expect to have when you submit the SAR to your organization:

- The information that is being collected about you
- The purpose of the information being collected
- Who the organization shares your data with
- How long the organization will store that data

From the mobile application side, by default when unplugged, ArcGIS Field Maps and ArcGIS QuickCapture attempts to upload your tracks approximately every 10 minutes. When plugged in and when the device has a battery charge of >= 20 percent, it will increase the upload frequency to 60 seconds. Separately, the last known location of the mobile user is updated every 60 seconds.

Removing Tracks from a Mobile Device

When a user signs out of Field Maps, QuickCapture, or Indoors, the tracks are removed from the device. Other users who use the app on the device don't have access to the tracks of previous users.

6 Conclusion

At Esri, confidentiality, integrity, and availability of information are priorities. Every technology use case is met with skepticism until its real value is discovered and understood by end users, organizations, or society. This has been true and more significant in recent years as the general population's privacy awareness has increased. Society has started treating data privacy and security as key issues with regard to any technology, products, and services that are offered to them. Concerns are even more elevated when it comes to location sharing services. To provide assurance, one needs to first understand what the concern is and why it is raised. As a customer, you need to be assured that the power to share privacy information still rests with you regardless of the technology, and Esri is committed to delivering that assurance.

The Software Security & Privacy team would like to give a note of thanks for the broad input and reviews from fellow teams at Esri, customers, and distributors. Esri intends to update this document in the future, so feel free to provide your comments and suggestions to *SoftwareSecurity@Esri.com*.

7 Frequently Asked Questions

- **What are the retention periods for user profile data?**
    - *The answer to this question depends on whether the administrator has enabled Esri access on the ArcGIS Online member account in question.*
        - *If Esri access is* ***not*** *enabled—Profile data exists as long as your organization persists or until the administrator or user deletes the profile information.*
        - *If Esri access is enabled—The member's full name, username, and email address are then pushed out to an Esri profile, which remains independent of the ArcGIS Online organizational account. To delete an Esri profile, the user would need to contact Esri Support Services.*
- **How is ArcGIS Online user profile information affected by a customer's SAML integration?**
    - *SAML integration with ArcGIS Online does not require population of the Esri profile. How profile information is handled is determined by the Esri access option chosen by the administrator, as discussed above.*
- **If an employee with a user account leaves an organization, and the email is removed from the customer's SAML IdP, is the corresponding ArcGIS Online account automatically deleted?**
    - *No, when a user is deleted from the SAML IdP, the user's account is not automatically deleted from* ArcGIS Online. *The SAML IdP will no longer let the user log in, but the user and any associated profile data will still exist within* ArcGIS Online *until an* ArcGIS Online *administrator deletes the* ArcGIS Online *account (at which point the discussion on Esri access vs. no access will apply).*
    - *If the employee in question never had Esri access enabled within ArcGIS Online, the profile information was never pushed out to an Esri profile; therefore, when the user account is deleted, their ArcGIS Online profile information is also deleted. If the employee had Esri access enabled and they want to delete their Esri profile data, they will need to contact support to remove it.*
- **What steps should be considered part of procedures for an employee who was using location sharing and is now leaving?**
    1. *Disable user's account—Ideally, your organization is utilizing SAML, and this function will be taken care of when the IT team disables the account on the Identity Provider System.*
    2. *Clear device data—If the device is owned by the employer, the employer can collect the device, but if the phone belongs to the employee, either utilize an MDM offering to force deleting the ArcGIS apps using location sharing and associated data or confirm that the user logs out of the device to clear local data.*
    3. *Confirm data value—If there is no business case for the data, it should be deleted with the tools, as described in section* 4.7.
- **What should a user do if they collected tracks during non-work hours that they would like deleted?**
    - *If the user has not yet uploaded the tracks from the mobile device, they can just sign out to delete all data not uploaded so far. If the data has already been synced, they should contact their administrator to use the delete tools discussed in section* 4.7.
- **How can I minimize exposure of user profile (personal) data?**
    - ArcGIS Enterprise *customers can disable the ArcGIS Portal Directory; otherwise, user information, such as Full name, First Name, Last Name, Username, and likely even employer information, can be found on the home page.*

    - *Be aware that the* profile *First Name and Username fields are exposed publicly no matter what the settings are if you allow publicly sharing data for your organization.*
- **Can my organization automatically start and stop location sharing on my device?**
    - *No. The mobile user is in complete control of when they are recording and sharing their location with others.*
- **Where does Esri store web service application customer data by default?**
    - *Much of the applications included in the ArcGIS system utilize ArcGIS Online and therefore store data within the United States. There is an option for regional data hosting in the United States, Europe and Asia-Pacific with ArcGIS Online. Most applications allow an organization to store their data within their ArcGIS Enterprise deployment, which can be located* in your country of choice.
- **What privacy laws govern my data?**
    - *See the Esri Master Agreement, section B 9.12 within the Trust Center Documents.*
- **Are there restrictions on what type of data I should store within ArcGIS Online?**
    - *Every customer has different security requirements associated with different data types or specific industry requirements. Esri recommends that customers not store sensitive personal data within ArcGIS Online unless it is encrypted or pseudonymized before posting it to be stored within our systems. A security gateway can be used to perform this function on the fly for your organization. If your organization requires Esri to view the information by providing us with the encryption key, please contact us at* SoftwareSecurity@esri.com *to ensure explicit consent is in place first.*
- **How can I most effectively archive tracks?**
    - *Python scripts*
- **How can I recover tracks if they are deleted?**
    - *Information concerning how to back up and restore the spatiotemporal big data store information may be found in the* product documentation: *enterprise.arcgis.com/en/portal/latest/administer/windows/data-store-backups.htm*
- **How are location tracks shared with others?**
    - *The location sharing service uses ownership-based access control to secure the tracks. Users can see only their own tracks unless they are an administrator or are assigned a role that contains a new View location tracks content privilege. This privilege allows a named user to view the tracks of others when accessing the tracks though a track view. Any administrator in your organization can use the Track Viewer web app to create track views. A track view consists of a list of mobile users that are being tracked along with additional named users that have the privilege to view the tracks of others (supervisors). Supervisors are given access to this track view through a group created by the Track Viewer web app. A track view is essentially a feature service view that can be used throughout the ArcGIS system for visualization and analysis.*

8 Additional Resource Information

8.1 ArcGIS Security and Privacy Best Practice Configuration Settings

Security and privacy assurance of a location sharing system is a shared responsibility between Esri and the customer. Whether you deploy and fully manage an ArcGIS Enterprise deployment, or utilize our SaaS offering ArcGIS Online, there are numerous settings that can affect both your organizations security and privacy posture overall. In the last several years, Esri has released tools to scan for key security concerns against customer deployments: 1) Python-based scripts for ArcGIS Server/Portal and 2) the Security Advisor, built into the ArcGIS Trust Center for ArcGIS Online. In writing this paper, we recognize that some settings have more significant privacy concerns then security concerns and sometimes vice-versa, that is not captured by the tools we have available today.

As part of our FedRAMP authorization for ArcGIS Online we created a customer responsibility list that customers can obtain from Esri. However, we realized that it would be even more helpful to provide our customers not only an understanding of the options, but also relative indicators for how much the options affect either security or privacy. On the next page we have created a table for customer administrators that lays out our recommended settings for products to minimize privacy and security risks for your operations. Some recommendations require additional components for the customer to acquire and implement, such as for enforcing data storage encryption of ArcGIS Enterprise, indicated by an answer of No for the column "Provided by Esri". Whether or not a setting is turned on by default as part of a new install is also listed (ArcGIS Enterprise the settings are based on 10.7.1). We indicate if the customer can configure/change the setting and we provide awareness of which settings our security validation tools check for, whether the Python-ArcGIS Enterprise scan scripts (Scan.py) or the ArcGIS Online Security Advisor (AGO SA).

We've aligned our relative security impact columns in the table with our security tools, and we will be adding a privacy assessment ranking to the Security Advisor later this year to further automate the validation process. We welcome your feedback on the recommendations and the current impact levels listed.

Topic	*Recommended Option*	ArcGIS Enterprise - 11 Base Deployment						ArcGIS Online				Criticality / Impact	
HTTPS and Encryption		*Provided by Esri*	*Default*	*Configurable*	Portal Scan	Server Scan	Security Advisor	*Provided by Esri*	*Default*	*Configurable*	Security Advisor	*Privacy*	*Security*
	Sitewide HTTPS TLS 1.2 and 1.3 Only	Yes	Yes	Yes	PS04	SS01	Yes	Yes	Yes	Yes	Yes	Danger	Danger
	Enforce HTTPS via HSTS	Yes	No	Yes	-	-	-	Yes	Yes	No	-	Warning	Warning
	Configure Preferred Encryption Algorithms	Yes	Yes	Yes	-	-	-	Yes	Yes	No	-	Warning	Warning
	Website endpoint CA Certificates	No	No	Yes	-	-	-	Yes	Yes	No	-	Danger	Danger
	CA Certificates used by Organization specific Identity Provider	No	No	Yes	-	-	-	No	No	Yes	-	Info	Info
	Enforce data storage encryption (1)	No	No	Yes	-	-	-	Yes	Yes	No	-	Danger	Danger
	Remove self signed certs	Yes	No	Yes	PS08	SS14	-	Yes	Yes	No	-	Warning	Info
	LDAP Identity Store communication encrypted	Yes	No	Yes	PS07	SS13	-	N/A	N/A	N/A	N/A	Info	Info
	Web Adaptor server uses HTTPS (2)	Yes	Yes	Yes	-	SS10	-	N/A	N/A	N/A	N/A	Danger	Danger
HTTP Header Config													
	X-Content-Type-Options: NOSNIFF	Yes	Yes	Yes	-	-	-	Yes	Yes	No	-	Warning	Warning
	X-XSS-Protection	Yes	Yes	No	-	-	-	No	No	No	-	Info	Info
	X-Frame-Options: SameOrigin	Yes (3)	Yes	No	-	-	-	Yes	Yes	No	-	Warning	Warning
Interfaces													
	Disable ArcGIS Services Directory	Yes	No	Yes	-	SS07	-	No	No	No	-	Warning	Warning
	Disable ArcGIS Portal Directory	Yes	No	Yes	PS03	-	-	Yes	Yes	No	-	Warning	Warning
	Limit access to ArcGIS Server Admin Resources via Web Adaptor	Yes	No	Yes	-	-	-	N/A	N/A	N/A	N/A	Warning	Warning
	Understand Dynamic Workspace usage	Yes	Yes	Yes	-	SS09	-	No	No	No	-	Warning	Warning
	Secure System Services	Yes	Yes	Yes (4)	-	SS06	-	Yes	Yes	No	-	Danger	Danger
Standardized Filtering													
	Enforce Standardized Queries	Yes	Yes	Yes	-	SS02	Yes	Yes	Yes	Yes	Yes	Danger	Danger
	Filter Web Content Enabled	Yes	Yes	Yes	-	SS05	-	Yes	Yes	No	-	Danger	Danger
Authentication and Authorization													
	Utilize Enterprise Logins via SAML instead of Built-in	No	No	Yes	-	-	Yes	No	No	Yes	Yes	Warning	Warning
	Block members joining org with social network credentials	No	No	No	-	-	Yes	Yes	No	Yes	Yes	Warning	Warning
	Define a password Complexity Policy	Yes	Yes	Yes	-	-	Yes	Yes	Yes	Yes	Yes	Warning	Danger
	Use Organinization Specific user store with account lockout policy	Yes	Yes	Yes	-	-	-	Yes	Yes	Yes	-	Warning	Warning
	Configure a shorter token Expiration Period	Yes	Yes	Yes	-	-	-	Yes	Yes	Yes	-	Warning	Warning
	Configure Multi-factor Authentication	Yes (5)	No	Yes	-	-	Yes	Yes	No	Yes	Yes	Danger	Danger
	Disallow user account self-creation	Yes	Yes	Yes	PS05	-	-	Yes	Yes	Yes	-	Warning	Danger
	Define Custom Roles	Yes	No	Yes	-	-	-	Yes	No	Yes	-	Warning	Warning
	Disable Anonymous Access to Portal home app	Yes	No	Yes	PS06	-	Yes	Yes	No	Yes	Yes	Danger	Warning
	Configure role based access control	Yes	Yes	Yes	-	-	-	Yes	Yes	Yes	-	Danger	Danger
	Disable Primary Site Administrator account (ArcGIS Server)	Yes	No	Yes	-	SS11	-	N/A	N/A	N/A	N/A	Warning	Warning
	Disable Initial Admin Account (Portal for ArcGIS)	Yes	No	Yes	-	-	-	N/A	N/A	N/A	N/A	Warning	Warning
	Disallow token generation in via GET	Yes	Yes	Yes	PS02	SS03	-	Yes	Yes	No	-	Danger	Danger
	Disallow token generation w/ creds in query parameter via POST	Yes	Yes	Yes	PS02	SS04	-	Yes	Yes	No	-	Danger	Danger
	SAML: Check if encrypted assertions and signed requests are enabled	Yes	No	Yes	PS13 (6)	-	-	Yes	No	Yes	-	Danger	Danger
ArcGIS Enterprise Web Tier Technologies													
	Use a WAF/Web Filter	No	No	Yes	-	-	-	Yes	Yes	No	-	Warning	Warning
	Utilize load balancer instead of Web Adaptor	No	No	Yes	-	-	-	Yes	Yes	No	-	Info	Warning
	Web Adaptor utilized for IWA only inside organization	Yes	Yes	Yes	-	-	-	No	No	No	-	Info	Info
	Remove Technology identifiers and banners	Yes	Yes	Yes (7)	-	-	-	Yes	Yes	No	-	Info	Info
	Use Data Loss Prevention (DLP)	No	No	Yes	-	-	-	Yes	-	-	-	Warning	Warning
Data Ownership & Privacy													
	Prevent users from sharing publicly	Yes	Yes	Yes	PS12	-	Yes	Yes	Yes	Yes	Yes	Warning	Warning
	Disallow biography edits and visibile profiles	Yes	Yes	Yes	-	-	Yes	Yes	Yes	Yes	Yes	Warning	Info
	Limit search to your organization only	Yes	Yes	Yes	-	-	Yes	Yes	No	Yes	Yes	Info	Info
	Remove social media links in item details/group pages	Yes	Yes	Yes	-	-	Yes	Yes	Yes	Yes	Yes	Warning	Info
	Do not allow members of other organizations to sign in	No	No	No	-	-	-	Yes	No	Yes	-	Warning	Warning
	Define specific allowed Portals that your Portal may access	Yes	No	Yes	-	-	-	Yes	No	Yes	Yes	Warning	Warning
	Validate Distributed Collaborations	Yes	No	Yes	-	-	-	Yes	No	Yes	-	Warning	Danger
	Disable Esri User Experience Improvement Program (EUEI)	No	No	No	-	-	-	Yes	No	Yes	Yes	Warning	Info
	Identify Authoritative Content (8)	No	No	No	-	-	-	Yes	No	Yes	-	Warning	Info
	Configure Access Notice	Yes	No	Yes	-	-	-	Yes	No	Yes	-	Info	Warning
	System Services Shared as portal item	Yes	Yes	Yes	-	SS15	-	-	-	-	-	Info	Info
	Validate Public Feature Services with update or delete permissions	Yes	Yes	Yes	-	SS12	-	Yes	Yes	Yes	Yes	Warning	Warning
Server Trust Relationships													
	Define servers for web tier authentication	Yes	No	Yes	-	-	-	Yes	No	Yes	Yes	Warning	Warning
	Define allowed proxy hosts	Yes	No	Yes	PS01	-	-	Yes	No	No	-	Warning	Warning
	Define Cross Origin Policy	Yes	No	Yes	PS09	SS08	-	Yes	No	Yes	Yes	Warning	Warning
	Federated server administrative URL	Yes	No	Yes	PS10	-	-	N/A	N/A	N/A	N/A	Warning	Danger
	Federated server services URL	Yes	No	Yes	PS11	-	-	N/A	N/A	N/A	N/A	Info	Info
Sharing Best Practices (9)													
	Create and document content review policy	No	No	Yes	-	-	-	No	No	Yes	-	Danger	Warning
	Create and document sharing review policy	No	No	Yes	-	-	-	No	No	Yes	-	Danger	Warning
	Validate need for editable layers	Yes	No	Yes	-	-	-	Yes	No	Yes	-	Danger	Warning

Figure 19 - ArcGIS Security and Privacy Recommended Settings

We define the three Criticality/Impact levels as follows for the recommended settings in Figure 19 as:

- **Danger** – Red – It should be extraordinarily rare to configure this setting for something other than the recommendation
- **Warning** – Yellow – There should be a clear business driver for utilizing a setting other than the recommended one, if not, implement the recommended setting
- **Info** – Blue – Risk level not major, but if you can shift to the recommended setting, you should.

Figure 19 notes:

1. In ArcGIS Enterprise, achieved via full disk encryption (e.g.: BitLocker)
2. Portal for ArcGIS, Web Adaptor must support HTTPS
3. X-Frame-Options: SameOrigin set on all login forms
4. By default, the System folder of services is only accessible to site publishers and administrators.
5. MFA provided natively OR via organization specific login provider
6. Upcoming ArcGIS Enterprise 11.1
7. User-configurable at Web Tier
8. Customers may opt into Authoritative Org program
9. Sharing policies are internally developed by the customer

8.2 Esri User Experience Improvement (EUEI)

Esri works continually to improve its products, and one of the best ways to find out what needs improvement is through customer feedback. The Esri User Experience Improvement program allows all Esri customers to contribute to the design and development of ArcGIS. EUEI collects information about how customers use ArcGIS and some of the problems that they encounter. Participation in EUEI is completely voluntary, and its usage should be reviewed as part of a customer's Privacy Impact Assessment (PIA):

- ArcGIS Online EUEI details—support.esri.com/en/technical-article/000016235
- ArcGIS Online FAQ—doc.arcgis.com/en/arcgis-online/reference/faq.htm
- *ArcGIS Blog* post: Importance of ArcGIS Online EUEI—esri.com/arcgis-blog/products/arcgis-online/uncategorized/you-can-impact-the-design-of-arcgis-online-with-just-a-click/?rmedium=redirect&rsource=blogs.esri.com%2Fesri%2Farcgis%2F2017%2F06%2F26%2F80818
- ArcGIS Desktop EUEI details—support.esri.com/en/technical-article/000011271

8.3 Additional Data Source Considerations

This section provides additional details about the various location sharing technologies that were introduced in section 2.4 of this paper, along with privacy considerations for each.

Beacons

Beacons are small hardware transmitters powered by batteries, which can be placed at a known location (indoors or outdoors). They use Bluetooth Low Energy (BLE) to broadcast a universally unique identifier (UUID) at regular intervals of time to nearby devices within a given range. BLE is very similar to Wi-Fi in the sense that it allows devices to communicate with each other. Beacons do not access or store information; they simply transmit information. BLE is ideal for situations where battery life is preferred over high data transfer speeds, such as indoor navigation. Due to the low power and short range, many overlapping beacons are needed to cover an area of interest.

Beacons come in two variances; *active* and *passive*. An active beacon has an internal power source (typically battery powered) to transmit data (see figure 20). BLE is used to help preserve the battery life of these devices. The most common use case for active beacons is real-time location sharing where several beacons allow for precision triangulation of location.

A *passive* beacon has no internal power source; it gets its power from electromagnetic energy that is transmitted to it. Once the beacon is powered, it will broadcast a UUID. The most common use case for passive beacons is in access control functions, such as key card access control systems.

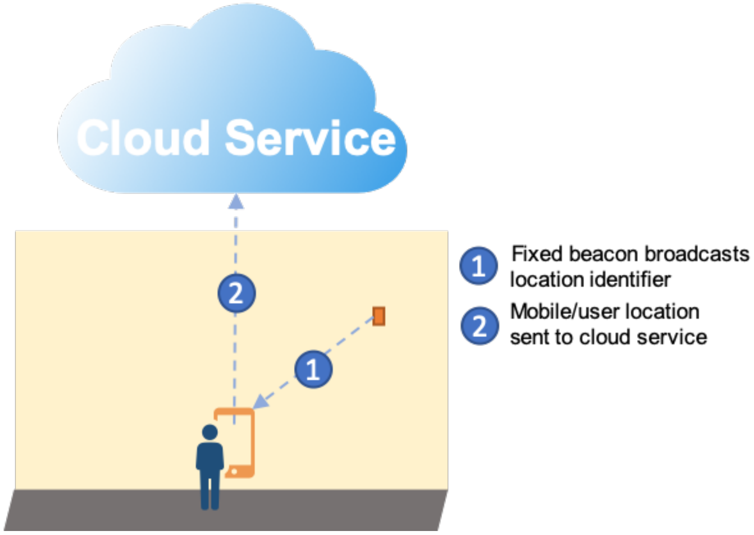

Cloud Service
2
1
1 Fixed beacon broadcasts location identifier
2 Mobile/user location sent to cloud service

Figure 20 – Building Beacon ID Received by Phone

Beacons have the following advantages:

- No PII transmitted, just the beacon's universally unique identifier (UUID)
- Lowest power drain on user devices utilizing low power Bluetooth
- More accurate than other data sources

Risks/Drawbacks associated with beacons are the following:

- Unlawful surveillance
- Receipt of unsolicited/undesired targeted advertisements
- Imprecise reporting of location

Receivers

These devices are mounted to permanent fixtures and continuously monitor the environment for beacons or other BLE signals, such as from a user's phone. When a tagged asset is nearby, the BLE receiver broadcasts this information back to a cloud service via Wi-Fi or cellular data. Advantages include that a mobile application is not required, and more frequent readings can be taken without draining devices. Disadvantages include higher installation costs and that it is considered more invasive by the resources being monitored, as they can no longer directly manage when they are being monitored.

Additional privacy concerns with receivers were discussed in section 2.5 and are shown in a typical deployment in figure 21. An overview of different scenarios for utilizing BLE beacons and receivers may be found at https://blog.lighthouse.io/exploring-new-ways-to-use-beacons-for-people-and-asset-tracking/.

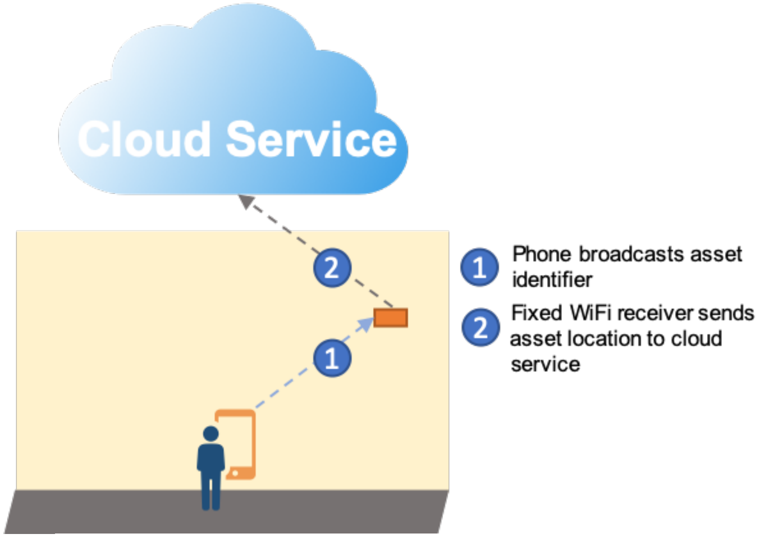

Cloud Service
2
1
1 Phone broadcasts asset identifier
2 Fixed WiFi receiver sends asset location to cloud service

Figure 21 - Building Receiver Capturing Phone ID

Unlawful Surveillance Risk

Location information or data submitted by beacons can be utilized not only by legitimate software applications but also by malware programs, which can provide criminals with access to information about an individual's location, hence leading to privacy concerns. Keep in mind that this is true for other data sources as well. Some mitigation options are below:

- Always require MFA on all application access.
- Limit application access to your resources through AppID—Oauth2 authorization.
- Conduct periodic audits against all applications accessing your solution in order to identify possible unauthorized surveillance applications.

Risk of Receiving Unsolicited/Undesired Targeted Advertisements

Many people, if not all, simply agree to the terms and conditions and the privacy policies of mobile applications without even reading them. Therefore, most would never intentionally agree to a legal provision in the application's privacy policy stating that the operation of the beacon may collect location data from beacons and pass it on to a third party that might send them advertisements.
Some of the mitigation options that can be leveraged in this case are as follows:

- Submit a request to opt out of any undesired feeds.
- Disable personalized ads in your browser.
- Unsubscribe from unsolicited mail through the Data & Marketing Association (DMA) website.

Location Reported May Not Be Precise Enough

If utilizing simple proximity detection, beacons are a good option; however, accuracy is seldom better than +/- 2 or 3 meters, and beacons do not provide an exact location. Some mitigation options are as follows:

- Place the beacons evenly within your environment—create zones.
- Make sure there is always a clear line of sight between the user's device and the beacons.

Wi-Fi

Wi-Fi powered location-based services use existing Wi-Fi infrastructure to detect the devices whose Wi-Fi is turned on. Wi-Fi can work in conjunction with GPS. Frequently, this is referred to as a Wi-Fi Positioning System (WPS), and it is particularly useful in urban areas or subways where GPS by itself is inadequate.

Wi-Fi can be provided either through the organization or a publicly accessible Wi-Fi. For most organizations, use of their Wi-Fi has implied consent on the end user's side, and users have full control on the decision to turn on/off location sharing on their device while on Wi-Fi, depending on the privacy banners and Wi-Fi provider's terms of use.

Depending on the type of Wi-Fi you are using—whether public, private, or organizational—there are privacy risks that should be considered. Publicly accessible Wi-Fi usually is not over encrypted channels, since most public Wi-Fi routers still have the default factory settings where encryption is turned off by default. So the possibility of snooping and sniffing of traffic over these public networks varies, which can affect your privacy.

Guidelines to ensure privacy when using Wi-Fi networks are as follows:

- Avoid automatically connecting to public Wi-Fi.
- Always verify that the connections are via HTTPS with TLS 1.2.
- Disable Wi-Fi capability when not in use.
- Use a VPN to ensure privacy over public Wi-Fi connections.

GPS

GPS is a satellite-based navigation system that has aided in the increased use of smartphones today, which, in turn, have led to the increased adoption of location-based services. GPS today is a first-class citizen in many end-users' lives as well as organizations' daily operations. GPS can be integrated into a mobile device or added as an external GPS.

GPS technology does not go without challenges. One of the most common challenges with location-based services using GPS is that GPS can be spoofed. This raises privacy concerns with LBS. So what can organizations do to guard against GPS spoofing? Below are some of the actions that can be taken to detect GPS spoofing.

Data Spike Detection

When an abnormally high number of location signals for a location are detected, they should be assessed, and if deemed inaccurate, the spikes should be removed from the location data. It is recommended to create a baseline as a starting point to help distinguish data spikes from normal usage.

Data Pattern Analysis

To better understand normal data patterns, a baseline must be set first. This requires some initial legwork to understand what normal data patterns look like so that when anomalies are detected, your team has something to compare them with. For example, if you have perfectly shaped lines or boxes as tracked data in your data collection, this type of data is not accurate as a real movement pattern, since no one would move in perfect squares or lines. When this analysis is made and this pattern is detected, it should be compared to the baseline and then removed once it is deemed incorrect.

8.4 Esri Privacy References

ArcGIS Trust Center Privacy Tab
trust.arcgis.com/en/privacy/privacy-tab-intro.htm

Initial Esri GDPR Commitment Statement
esri.com/arcgis-blog/products/product/administration/esris-committment-to-gdpr-privacy-security/

Magazine Article Discussing GDPR and GIS
www.gis-professional.com/files/8bd7fa6f53134780c0310a1fff7980e3.pdf

The Privacy Paradox: How Companies Gain Consumer Confidence in Data Sharing
esri.com/about/newsroom/publications/wherenext/privacy-paradox-and-location-sharing/

9 Acronyms

This section lists acronyms that are used in this technical paper:

- 3PAO: Third-Party Assessment Organization
- AD: Active Directory
- API: Application Program Interface
- ATO: Authority to Operate
- AWS: Amazon Web Services
- BLE: Bluetooth Low Energy
- CA: Certificate Authority
- CAIQ: Consensus Assessment Initiative Questionnaire
- CCPA: California Consumer Privacy Act
- CPRA: California Privacy Rights Act
- CIPT: Certified Information Privacy Technologists
- CIS: Center for Internet Security
- CISO: Chief Information Security Officer
- CPO: Chief Privacy Officer
- CSA: Cloud Security Alliance
- CSV: Comma-Separated Value
- DAC: Discretionary Access Control
- DLP: Data Loss Prevention
- DPA: Data Processing Addendum
- DPO: Data Privacy Officer
- DISA: Defense Information Systems Agency
- DMZ: Demilitarized Zone
- ETL: Extract, Transform, and Load
- EU: European Union
- EUEI: Esri User Experience Improvement
- FedRAMP: Federal Risk and Authorization Management Program
- GDPR: General Data Protection Regulation
- GIS: Geographic Information System
- GPS: Global Positioning System
- HSTS: HTTP Strict Transport Security
- HTTP: Hypertext Transfer Protocol
- HTTPS: Secure Hypertext Transfer Protocol
- IAPP: International Association of Privacy Professionals
- ICO: Information Commissioner's Office
- IdP: Identity Provider
- IPsec: Internet Protocol Security
- IT: Information Technology
- JDBC: Java Database Connectivity
- KMS: Key Management System
- LDAP: Lightweight Directory Access Protocol
- LBS: Location-Based Service
- LKL: Last Known Location
- MDM: Mobile Device Management
- MFA: Multifactor Authentication

- MITM: Man-in-the-Middle
- NDA: Non-Disclosure Agreement
- NAS: Network-Attached Storage
- OBAC: Ownership-Based Access Control
- OWASP: Open Web Application Security Project
- PbD: Privacy by Design
- PHI: Protected Health Information
- PIA: Privacy Impact Assessment
- PII: Personally Identifiable Information
- RDP: Remote Desktop Protocol
- RTO: Recovery Time Objective
- SaaS: Software as a Service
- SAML: Security Assertion Markup Language
- SAR: Subject Access Request
- SDK: Software Development Kit
- SIEM: Security Information and Event Management
- SLA: Service-Level Agreement
- SSH: Secure Shell
- STIG: Security Technical Implementation Guide
- TLS: Transport Layer Security
- UUID: Universally Unique Identifier
- VPN: Virtual Private Network
- WAF: Web Application Firewall
- WPS: Wi-Fi Positioning System
- XML: Extensible Markup Language

10 Definitions

California Consumer Privacy Act of 2018 (CCPA) – A law effective as of January 1, 2020 intended to enhance privacy rights and consumer protection for residents of California, United States. The CCPA fact sheet provides additional detail.

Data controller—A natural or legal person (such as a member of an organization) who (either alone or with others) determines the purposes and means of the processing of the personal data.

Data processor or Service Provider—A natural or legal person who processes personal data on behalf of a data controller

Data subject—An identified or identifiable living individual who can be identified, directly or indirectly, by reference to an identifier or information or other factors relating to the individual.

Encryption—Obscures information by replacing identifiers with something else. But whereas pseudonymization allows anyone with access to the data to view part of the data et, encryption allows only approved users to access the full dataset. Note that pseudonymization and encryption can be used simultaneously or separately.

Explicit consent—Similar to GDPR's standard requirements for obtaining consent, the difference is that it must be obtained in a way that leaves no room for misinterpretation. This means it must be provided in a clear statement—whether written or spoken. An explicit consent statement will also need to specifically refer to the element of the processing that requires explicit consent. For example, as the Information Commissioner's Office (ICO) states, "the statement should specify the nature of data that's being collected, the details of the automated decision and its effects, or the details of the data to be transferred and the risks of the transfer."

General Data Protection Regulation (GDPR) —A regulatory framework that sets legal requirements for the collection and processing of personal information from individuals who live in the European Union. More information about GDPR can be found at https://gdpr.eu/what-is-gdpr/.

Location sharing—Technology that physically locates and electronically records and tracks the movement of people or objects. Esri provides mobile applications that include collecting location information and storing it in customer-managed deployments of ArcGIS Enterprise or Esri's managed software-as-a-service offering ArcGIS Online for analysis by the customer.

Personal data—Any information relating to a data subject, such as their name or address.

Pseudonymization—Masks data by replacing identifying information with artificial identifiers. Although it is central to protecting data—being mentioned 15 times in the GDPR—and can help protect the privacy and security of personal data, pseudonymization has its limits, which is why the GDPR also mentions encryption.

Spatiotemporal big data store—A NoSQL database used for storing feature service data (such as location data) and which is available with the ArcGIS Data Store product. The spatiotemporal big data store enables archival of high-volume locational data, sustains high-velocity write throughput, and can run across multiple machines.

esri | THE SCIENCE OF WHERE™

Esri, the global market leader in geographic information system (GIS) software, offers the most powerful mapping and spatial analytics technology available.

Since 1969, Esri has helped customers unlock the full potential of data to improve operational and business results. Today, Esri software is deployed in more than 350,000 organizations including the world's largest cities, most national governments, 75 percent of Fortune 500 companies, and more than 7,000 colleges and universities. Esri engineers the most advanced solutions for digital transformation, the Internet of Things (IoT), and location analytics to inform the most authoritative maps in the world.

Visit us at esri.com.

Contact Esri

380 New York Street
Redlands, California 92373-8100 USA

1 800 447 9778
T 909 793 2853
F 909 793 5953
info@esri.com
esri.com

Offices worldwide
esri.com/locations

For more information, visit Trust.ArcGIS.com.