**IUP.2** Information Use Practices [IUP]

Invisible AI training data collection. You are forceably made to help train computer vision every time you interact with an AI system. This is similar to IUP.2, but in this case, the Service Provider is the software, not an individual. You have expectations and/or grant explicit permissions about how you want your information used. However, the Service Provider is required to respect your privacy preferences, but they are not bound by any legal requirement to do so. You have no control over how your information is used by the software.

**IUP.1**

Sharing individual’s information with non-Data Processors.

In the shopping example above, you have configured your settings to not allow your information to be shared with 3rd parties for the purpose of providing targeted advertisements. You have selected a product from a competitor Datalogix match offline databases to online data, which has no bearing on nearly all services, where “Single” is available. Even though the individual may only be shared with 3rd parties for the purpose of providing the service, the individual must be regarded as a Data Processor as defined in the applicable law. The individual may be regarded as a Data Processor in some cases, even if the individual is not explicitly identified or associated with people, products and services they may not necessarily be interested in.

**ISP.1** Information Sharing Practices [ISP]

You have a right to know who has access to your personal information. You have the right to know how your personal information is being used and what kind of information is being collected. This is a requirement to fulfill the transaction. You've selected a product from a competitor Datalogix match offline databases to online data, which has no bearing on nearly all services, where “Single” is available. Even though the individual may only be shared with 3rd parties for the purpose of providing the service, the individual must be regarded as a Data Processor as defined in the applicable law. The individual may be regarded as a Data Processor in some cases, even if the individual is not explicitly identified or associated with people, products and services they may not necessarily be interested in.

**ICP.8** Information Collection Practices [ICP]

The practice of invisible AI training data collection. You are forceably made to help train computer vision every time you interact with an AI system. This is similar to IUP.2, but in this case, the Service Provider is the software, not an individual. You have expectations and/or grant explicit permissions about how you want your information used. However, the Service Provider is required to respect your privacy preferences, but they are not bound by any legal requirement to do so. You have no control over how your information is used by the software.
ISP.2

Companies use biometric information to enhance their services, which can lead to privacy concerns.

Inverse Privacy / Data Brokers [IPDB] Supplier Lock-In & Contracts of Adhesion [LICA]

Identity Practices [IDPR]

IDPR.1

IDPR.3 Loss or Misuse of acquired facial

platforms or other platforms for purchased hardware and time. (contracts of adhesion)

IDPR.4

loss of autonomy and agency. Victim of coercion.

ISP.2

companies gain assurance that biometric information is being used as intended. The storage of sensitive.

Privacy settings ([85], 2019)

Apple states “unauthorized modification of iOS is a violation of

Terms of Service by the end user to the TOS and Privacy Policy. Use TOS;DR

See video links and video content from private data

Vendors/Platforms do not facilitate direct "Save as PDF"/"Save as Image"/"Save as Text" functionality.

Vendors should allow user to create permissions and access restrictions for content posted on their account. See [10], page 42.

Apple states “unauthorized modification of iOS is a violation of

Terms of Service by the end user to the TOS and Privacy Policy. Use TOS;DR

See video links and video content from private data

Vendors/Platforms do not facilitate direct "Save as PDF"/"Save as Image"/"Save as Text" functionality.

Vendors should allow user to create permissions and access restrictions for content posted on their account. See [10], page 42.

Apple states “unauthorized modification of iOS is a violation of

Terms of Service by the end user to the TOS and Privacy Policy. Use TOS;DR

See video links and video content from private data

Vendors/Platforms do not facilitate direct "Save as PDF"/"Save as Image"/"Save as Text" functionality.

Vendors should allow user to create permissions and access restrictions for content posted on their account. See [10], page 42.

Apple states “unauthorized modification of iOS is a violation of

Terms of Service by the end user to the TOS and Privacy Policy. Use TOS;DR

See video links and video content from private data

Vendors/Platforms do not facilitate direct "Save as PDF"/"Save as Image"/"Save as Text" functionality.

Vendors should allow user to create permissions and access restrictions for content posted on their account. See [10], page 42.

Apple states “unauthorized modification of iOS is a violation of

Terms of Service by the end user to the TOS and Privacy Policy. Use TOS;DR

See video links and video content from private data

Vendors/Platforms do not facilitate direct "Save as PDF"/"Save as Image"/"Save as Text" functionality.

Vendors should allow user to create permissions and access restrictions for content posted on their account. See [10], page 42.

Apple states “unauthorized modification of iOS is a violation of

Terms of Service by the end user to the TOS and Privacy Policy. Use TOS;DR

See video links and video content from private data

Vendors/Platforms do not facilitate direct "Save as PDF"/"Save as Image"/"Save as Text" functionality.

Vendors should allow user to create permissions and access restrictions for content posted on their account. See [10], page 42.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>FTC.04</td>
<td>User controls the data they provide and how it is used</td>
<td>Users are more likely to trust and use a given system if they feel in control of the data they provide.</td>
<td>A user is more likely to trust and use a given system if they feel in control of the data they provide.</td>
<td>The user should have clear and visible options for how their data is used.</td>
<td>The user should have clear and visible options for how their data is used.</td>
<td>Users should be informed about data collection practices and have the ability to opt out of data sharing.</td>
<td>GDPR, CCPA, PIPEDA</td>
</tr>
<tr>
<td>FTC.05</td>
<td>Users have access to their data and can easily request its deletion</td>
<td>Users are more likely to trust and use a given system if they feel in control of the data they provide.</td>
<td>A user is more likely to trust and use a given system if they feel in control of the data they provide.</td>
<td>The user should have clear and visible options for how their data is used.</td>
<td>The user should have clear and visible options for how their data is used.</td>
<td>Users should be informed about data collection practices and have the ability to opt out of data sharing.</td>
<td>GDPR, CCPA, PIPEDA</td>
</tr>
<tr>
<td>FTC.06</td>
<td>Data is secure and protected against unauthorized access or disclosure</td>
<td>Data is less likely to be compromised if it is stored securely.</td>
<td>A user is more likely to trust and use a given system if they feel in control of the data they provide.</td>
<td>The user should have clear and visible options for how their data is used.</td>
<td>The user should have clear and visible options for how their data is used.</td>
<td>Users should be informed about data collection practices and have the ability to opt out of data sharing.</td>
<td>GDPR, CCPA, PIPEDA</td>
</tr>
<tr>
<td>FTC.07</td>
<td>Users are aware of the purpose of data collection and why it is necessary</td>
<td>Users are more likely to trust and use a given system if they feel in control of the data they provide.</td>
<td>A user is more likely to trust and use a given system if they feel in control of the data they provide.</td>
<td>The user should have clear and visible options for how their data is used.</td>
<td>The user should have clear and visible options for how their data is used.</td>
<td>Users should be informed about data collection practices and have the ability to opt out of data sharing.</td>
<td>GDPR, CCPA, PIPEDA</td>
</tr>
<tr>
<td>FTC.08</td>
<td>Users are provided with clear and transparent information about data practices</td>
<td>Users are more likely to trust and use a given system if they feel in control of the data they provide.</td>
<td>A user is more likely to trust and use a given system if they feel in control of the data they provide.</td>
<td>The user should have clear and visible options for how their data is used.</td>
<td>The user should have clear and visible options for how their data is used.</td>
<td>Users should be informed about data collection practices and have the ability to opt out of data sharing.</td>
<td>GDPR, CCPA, PIPEDA</td>
</tr>
<tr>
<td>FTC.09</td>
<td>Users are given the option to limit or control data collection and use</td>
<td>Users are more likely to trust and use a given system if they feel in control of the data they provide.</td>
<td>A user is more likely to trust and use a given system if they feel in control of the data they provide.</td>
<td>The user should have clear and visible options for how their data is used.</td>
<td>The user should have clear and visible options for how their data is used.</td>
<td>Users should be informed about data collection practices and have the ability to opt out of data sharing.</td>
<td>GDPR, CCPA, PIPEDA</td>
</tr>
<tr>
<td>FTC.10</td>
<td>Users are informed about the ways in which their data is used</td>
<td>Users are more likely to trust and use a given system if they feel in control of the data they provide.</td>
<td>A user is more likely to trust and use a given system if they feel in control of the data they provide.</td>
<td>The user should have clear and visible options for how their data is used.</td>
<td>The user should have clear and visible options for how their data is used.</td>
<td>Users should be informed about data collection practices and have the ability to opt out of data sharing.</td>
<td>GDPR, CCPA, PIPEDA</td>
</tr>
<tr>
<td>FTC.11</td>
<td>Users are given the option to limit or control data collection and use</td>
<td>Users are more likely to trust and use a given system if they feel in control of the data they provide.</td>
<td>A user is more likely to trust and use a given system if they feel in control of the data they provide.</td>
<td>The user should have clear and visible options for how their data is used.</td>
<td>The user should have clear and visible options for how their data is used.</td>
<td>Users should be informed about data collection practices and have the ability to opt out of data sharing.</td>
<td>GDPR, CCPA, PIPEDA</td>
</tr>
</tbody>
</table>


## Surveillance

---

**Surveillance [SURV]**

1. **Browser fingerprinting uniquely identifies individuals:**
   - Collects device characteristics, browser details, and other attributes.
   - Can be used to track users across different devices and sessions.

2. **Zombie Cookies, Flash Cookies & Permacookies:**
   - Cookies that persist even after browser is closed.
   - Can be used for tracking and data collection.

3. **Unreadable Terms of Service:**
   - TOS filled with legal and technical jargon.
   - Users often do not read them.

---

## Technology

---

**Technology [TECH]**

1. **Dark Patterns:**
   - A user interface that's designed to trick users.
   - Examples: obscured navigation, misleading language.

2. **Device fingerprinting:**
   - Collects information on a remote computing device.
   - Used for targeted advertising.

---

## Social Media

---

**Social Media [SOC]**

1. **Data ecosystem:**
   - As data贯ecomes more valuable, the data economy becomes more powerful.

2. **Collecting data on children:**
   - Children are particularly vulnerable to data collection.

---

## Legislation

---

**Legislation [LEG]**

1. **Algorithmic Accountability Act of 2019:**
   - Requires federal agencies to assess and mitigate the potential harms of algorithms.

2. **Online Copyright Infringement Liability Limitation Act (OCILLA):**
   - Protects online service providers from liability for copyright infringement.

---

## Additional Resources

---

**Resources:**

- Wikipedia articles on Zombie Cookies, Flash Cookies, and Permacookies.
- Website on browser fingerprinting.
- Article on Dark Patterns.
- Banker's guide to online gambling industry.

---

## Footnotes

---

1. [Source]

---

##Acknowledgments

---

*Note: The text is a compilation of various sources and perspectives on digital surveillance, technology, and privacy issues.*
Facial recognition is biased. "The Best Algorithms Struggle to Recognize Black Faces"

"Many large organizations rely on more than conclusions reached by opaque algorithms, and deny due process. Those metrics can be biased and used in a purely mechanical way.

Humans over-anthropomorphize key phrases, mathematically scoring them for relevance, and sending it as a better than your senses or intuition. In cases where you may have a good sense of your intention and goal, check to disable personalization, you may want to do so.

Although rare, there are situations where facial recognition can be problematic. For example, in law enforcement, facial recognition technology has been used to identify suspects.

A 2016 study by the National Institute of Standards and Technology (NIST) found that the accuracy of facial recognition systems varied widely, with some systems incorrectly identifying individuals of the same race as a different race.

In particular, the study found that facial recognition systems were less accurate for people with darker skin tones. The study also found that the accuracy of facial recognition systems improved when the training data included a more diverse group of people.

In general, the immediate implications for you is that information to discriminate against you may be being filtered. You receive filtered information based on whatever algorithms are in place by the search engine. Your version of reality and "truth" are place by the search engine. Your version of reality and "truth" are place by the search engine.

You may be being manipulated in ways you don't even know. The filtering of information only uses models.

Toxic language (e.g., hate speech, abusive speech, or other offensive language) can be further gather results, and can avalanche the relevant research. The research here is still pretty underdeveloped, which is a cause for concern. AI algorithms perpetuate racial bias in lending.

Be aware that personalized products can become increasingly targeted toward what they think you have the capacity for, the future you and the experience you're going to have.

The research here is still pretty underdeveloped, which is a cause for concern. AI algorithms perpetuate racial bias in lending.

Automation bias in intelligent time critical decision making: What is the impact of AI in the race for the sky? The rise of the autopilot plane.

Toxic language (e.g., hate speech, abusive speech, or other offensive language) can be further gathered results, and can avalanche the relevant research. The research here is still pretty underdeveloped, which is a cause for concern.

AI algorithms perpetuate racial bias in lending.

In particular, the study found that facial recognition systems were less accurate for people with darker skin tones. The study also found that the accuracy of facial recognition systems improved when the training data included a more diverse group of people.

In general, the immediate implications for you is that information to discriminate against you may be being filtered. You receive filtered information based on whatever algorithms are in place by the search engine. Your version of reality and "truth" are place by the search engine. Your version of reality and "truth" are place by the search engine.

In cases where you may have a good sense of your intention and goal, check to disable personalization, you may want to do so.

Although rare, there are situations where facial recognition can be problematic. For example, in law enforcement, facial recognition technology has been used to identify suspects.

A 2016 study by the National Institute of Standards and Technology (NIST) found that the accuracy of facial recognition systems varied widely, with some systems incorrectly identifying individuals of the same race as a different race.

In particular, the study found that facial recognition systems were less accurate for people with darker skin tones. The study also found that the accuracy of facial recognition systems improved when the training data included a more diverse group of people.

In general, the immediate implications for you is that information to discriminate against you may be being filtered. You receive filtered information based on whatever algorithms are in place by the search engine. Your version of reality and "truth" are place by the search engine. Your version of reality and "truth" are place by the search engine.

You may be being manipulated in ways you don't even know. The filtering of information only uses models.

Toxic language (e.g., hate speech, abusive speech, or other offensive language) can be further gather results, and can avalanche the relevant research. The research here is still pretty underdeveloped, which is a cause for concern. AI algorithms perpetuate racial bias in lending.

Be aware that personalized products can become increasingly targeted toward what they think you have the capacity for, the future you and the experience you're going to have.