# Digital Harms Dictionary
Produced by Internet Safety Labs

<table>
<thead>
<tr>
<th>Practice</th>
<th>Description of Digital Harm</th>
<th>Implications for You</th>
<th>Examples of Underlying Behavior</th>
<th>Corresponding References</th>
<th>What You Can Do Today</th>
<th>Where All-Side Recommendations for Victims</th>
<th>Legislation/Bills</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICP 1</td>
<td>Users are permitted to use a feature of the Digital Service in a manner not intended by the Service Provider.</td>
<td>Systems are collecting personal data and deciding to communicate with other parties.</td>
<td>Using certain software to manipulate data for personal benefit.</td>
<td>[20]</td>
<td>Learn about the feature in question.</td>
<td>[20]</td>
<td>- -</td>
</tr>
<tr>
<td>ICP 2</td>
<td>Gathering information about the individual’s and their behavior that is not intended by the Service Provider in a manner not intended by the Service Provider.</td>
<td>Using the system to access personal information.</td>
<td>Using the system to access personal information.</td>
<td>[20]</td>
<td>Avoid access to personal information.</td>
<td>[20]</td>
<td>- -</td>
</tr>
<tr>
<td>ISP 1</td>
<td>Systems are collecting personal data and are deciding to communicate with other parties.</td>
<td>Using the system to access personal information.</td>
<td>Using the system to access personal information.</td>
<td>[20]</td>
<td>Avoid access to personal information.</td>
<td>[20]</td>
<td>- -</td>
</tr>
</tbody>
</table>

---

**Note:** The table above provides a comprehensive overview of digital harms, their implications, underlying behaviors, corresponding references, actions you can take, and where all-side recommendations for victims can be found. The legislation/bills section lists relevant laws and regulations, which are crucial for understanding the legal frameworks governing these issues. For a detailed analysis of specific cases, such as Facebook allowing third-party use of my photo to advertise, or how DNA companies like Ancestry and 23andme are using your genetic information, the references in the table can be consulted. The table also includes links to resources for further reading, such as the Digital Harms Dictionary and the Digital Privacy and Security Act of 2019. Understanding these harms and their mitigation is essential for protecting digital privacy and security.
privacy practices [isp]
id description of digital

idpr.1
loss or misuse of acquired
hardware and software
configurations, though we
never read them. (and
never inspect the images and
videos that are being loaded on
the websites. but links in the emails
actually go to malicious sites,
emails pretending to be from an
acquaintance or official
sender. (ex. your bank)

idpr.2
 browsers and search engines,
when not storing biometric as a hash.

idpr.3
examine any data broker, such as acxiom, nielsen, experian,
experian, equifax

idpr.4
privacy settings/(
[85], 2019)

idpr.5
prices of digital

idpr.6
in current ongoing scams, criminals are sending phishing
e-mails pretending to be from an acquaintance or official
sender. (ex. your bank)

idpr.7
make the company's behavior to ensure they're doing what
they promised. (and)

idpr.8
as "friend" who has access to the info in a bounded
posting something in a limited exposure
space (only friends

idpr.9
users may not wish to disclose their marital status or
even associate

idpr.10
organizations, social networks, particularly facebook. this
information can be used to

idpr.11
banning practices
[isp]

idpr.12
"a centralized database can be used to track anyone's physical
presence or movements, not just

idpr.13
is working to create a universal, persistent and anonymized
solution. (ex. the social networking site twitter)

idpr.14
"...it can be commandeered by government bodies for use
against citizens.

idpr.15
"...gives the companies, not to mention the subjects of the data, even
more control over where it goes and how it is used.

idpr.16
industry's reliance on third-party cookies.

idpr.17
the online ad industry's reliance on third-party cookies.

idpr.18
...companies give assurances...that
the harm.

idpr.19
...the windows 10 default privacy settings leave a lot to be
desired. (ex. some info is transmitted to

idpr.20
...the windows 10 default privacy settings leave a lot to be
desired. (ex. some info is transmitted to

idpr.21
...it can be commandeered by government bodies for use
against citizens.

idpr.22
...gives the companies, not to mention the subjects of the data, even
more control over where it goes and how it is used.

idpr.23
industry's reliance on third-party cookies.

idpr.24
the online ad industry's reliance on third-party cookies.

idpr.25
...companies give assurances...that
the harm.

idpr.26
...the windows 10 default privacy settings leave a lot to be
desired. (ex. some info is transmitted to

idpr.27
...it can be commandeered by government bodies for use
against citizens.

idpr.28
...gives the companies, not to mention the subjects of the data, even
more control over where it goes and how it is used.

idpr.29
industry's reliance on third-party cookies.

idpr.30
the online ad industry's reliance on third-party cookies.

idpr.31
...companies give assurances...that
the harm.

idpr.32
...the windows 10 default privacy settings leave a lot to be
desired. (ex. some info is transmitted to

idpr.33
...it can be commandeered by government bodies for use
against citizens.

idpr.34
...gives the companies, not to mention the subjects of the data, even
more control over where it goes and how it is used.

idpr.35
industry's reliance on third-party cookies.

idpr.36
the online ad industry's reliance on third-party cookies.

idpr.37
...companies give assurances...that
the harm.

idpr.38
...the windows 10 default privacy settings leave a lot to be
desired. (ex. some info is transmitted to

idpr.39
...it can be commandeered by government bodies for use
against citizens.

idpr.40
...gives the companies, not to mention the subjects of the data, even
more control over where it goes and how it is used.

idpr.41
industry's reliance on third-party cookies.

idpr.42
the online ad industry's reliance on third-party cookies.

idpr.43
...companies give assurances...that
the harm.

idpr.44
...the windows 10 default privacy settings leave a lot to be
desired. (ex. some info is transmitted to

idpr.45
...it can be commandeered by government bodies for use
against citizens.

idpr.46
...gives the companies, not to mention the subjects of the data, even
more control over where it goes and how it is used.

idpr.47
industry's reliance on third-party cookies.

idpr.48
the online ad industry's reliance on third-party cookies.

idpr.49
...companies give assurances...that
the harm.

idpr.50
...the windows 10 default privacy settings leave a lot to be
desired. (ex. some info is transmitted to

idpr.51
...it can be commandeered by government bodies for use
against citizens.

idpr.52
...gives the companies, not to mention the subjects of the data, even
more control over where it goes and how it is used.

idpr.53
industry's reliance on third-party cookies.

idpr.54
the online ad industry's reliance on third-party cookies.

idpr.55
...companies give assurances...that
the harm.

idpr.56
...the windows 10 default privacy settings leave a lot to be
desired. (ex. some info is transmitted to

idpr.57
...it can be commandeered by government bodies for use
against citizens.

idpr.58
...gives the companies, not to mention the subjects of the data, even
more control over where it goes and how it is used.

idpr.59
industry's reliance on third-party cookies.

idpr.60
the online ad industry's reliance on third-party cookies.
<table>
<thead>
<tr>
<th>PRACTICE</th>
<th>ID</th>
<th>DESCRIPTION OF DIGITAL USE</th>
<th>IMPLICATIONS FOR YOU</th>
<th>EXAMPLES OF UNDESIRABLE BEHAVIOR</th>
<th>CONSIDERATION OF REFERENCES</th>
<th>WHAT YOU CAN DO TODAY</th>
<th>MORE ALLOCATION RECOMMENDATION FOR ANSWERS</th>
<th>LEGISLATION / BILL S</th>
</tr>
</thead>
<tbody>
<tr>
<td>EULA.4</td>
<td>The way to define an account, (not) automatically include account access in your internet connection, and may vary if not in all jurisdictions</td>
<td>Personally ability to have owned account access granted.</td>
<td>Privacy breaches from this &quot;I did not browse the web, we have cookies&quot; violation. On Twitter you can retrieve the Statement under &quot;You can access your...&quot; or &quot;appcrawler.tumblr.com&quot; and you can browse the items you have. To access your personal browser, you have to go through a login process. If the browser is not supported, the access may only include access to the data that is available.</td>
<td>Doesn't access to personal data such as your account, or account information is not</td>
<td>[5]</td>
<td>- Offer a套餐 enrollment at option. This service may access your personal account information. Make this clear to the user.</td>
<td>[6]</td>
<td>S.1108 - Algorithmic Accountability Act of 2019, S.3861 Exposure Notification Privacy Act, S.4626 - SAFE DATA Act, S.3861 Exposure Notification Privacy Act, S.3861 Exposure Notification Privacy Act</td>
</tr>
</tbody>
</table>
Practices and implications of undesired behavior

**Pract 1.1** Non-subjective social control and marketing technologies in smart devices

- **Implications for You**
  - People sign up for services (or create accounts) without knowing what they are agreeing to.
  - The term was created by Attorney Joseph H. Malley who initiated the Super-8 lawsuit.

- **Examples of Undesired Behavior**
  - Publicly available
  - Publicly available

- **Corresponding References**
  - "A zombie cookie is an HTTP cookie that is recreated after deletion. The term was coined by Attorney Joseph H. Malley when he filed the Super-8 lawsuit." [Wikipedia]

- **What You Can Do Today**
  - Don't use zombie cookies, flash cookies or permanent cookies. S.1108 - Algorithmic Accountability Act of 2019, S. 4400 National Notification Privacy Act

- **Legislation / Bills**
  - S.2355 - End Racial and Religious Profiling Act of 2019

---

**Pract 1.2** Surveys

- **Implications for You**
  - You may not even know you're participating in a survey.

- **Examples of Undesired Behavior**
  - Surveillance is applied racially.

- **Corresponding References**
  - "Surveillance is applied racially. Sometimes non-technical people, and suppliers of technology, are naturally obscure to the verification, demographic needs around data, and understandings of the Me2B deal taking place. Often, the term was created by Attorney Joseph H. Malley who initiated the Super-8 lawsuit." [Wikipedia]

- **What You Can Do Today**
  - Use Panopticlick, Privacy Badger or other TOSDR browser extension and https://pribot.org/polisis

- **Legislation / Bills**
  - S.4400 National Notification Privacy Act (2019)

---

**Pract 1.3** Consent

- **Implications for You**
  - Consent can be solicited through a variety of mechanisms.

- **Examples of Undesired Behavior**
  - Consent is solicited in an HTML form that never gets after the user.

- **Corresponding References**
  - "Canvas fingerprinting actually recognizes your browser of choice..." [EPICxx]

- **What You Can Do Today**
  - Use up to date security/scanning software

- **Legislation / Bills**
  - S.3861 Exposure Notification Privacy Act , S.2355 - End Racial and Religious Profiling Act of 2019

---

**Pract 1.4** Privacy policies

- **Implications for You**
  - Privacy policies are overly legal.

- **Examples of Undesired Behavior**
  - "A panel concluded that the photo was not a private event, but a public event..." [84], 2019

- **Corresponding References**
  - "The face and voice of servility and compliance..." [Kessler Page]

- **What You Can Do Today**
  - Use TOS analytical tools such as: TOSDR browser extension

- **Legislation / Bills**
  - S.2355 - End Racial and Religious Profiling Act of 2019

---

**Pract 1.5** Data collection

- **Implications for You**
  - Data collected without user's consent.

- **Examples of Undesired Behavior**
  - Don't do this. Minimize sensor usage.

- **Corresponding References**
  - "...African-American real estate agent who was stopped by police because neighbors thought it was 'suspicious' for him to be walking..." [Wikipedia]

- **What You Can Do Today**
  - Technology is naturally addictive.

- **Legislation / Bills**
  - S.3861 Exposure Notification Privacy Act

---

**Pract 1.6** Dark patterns

- **Implications for You**
  - Dark patterns are deliberate manipulation through the user interface.

- **Examples of Undesired Behavior**
  - Theophany has hired design experts out of the UC Berkeley School of Information.

- **Corresponding References**
  - "Dark patterns are deliberate manipulation through the user interface..." [Kessler Page]

- **What You Can Do Today**
  - Use apps and timers to limit technology use.

- **Legislation / Bills**
  - S.2355 - End Racial and Religious Profiling Act of 2019

---

**Pract 1.7** Gender stereotypes

- **Implications for You**
  - Gender stereotypes are reinforced.

- **Examples of Undesired Behavior**
  - "Gender stereotypes are reinforced..." [Wikipedia]

- **Corresponding References**
  - "Gender stereotypes are reinforced..." [Wikipedia]

- **What You Can Do Today**
  - Educate yourself and be mindful of when and how to proffer your own voice.

- **Legislation / Bills**
  - S.3861 Exposure Notification Privacy Act

---

**Pract 1.8** Dark patterns

- **Implications for You**
  - Dark patterns are deliberate manipulation through the user interface.

- **Examples of Undesired Behavior**
  - Theophany has hired design experts out of the UC Berkeley School of Information.

- **Corresponding References**
  - "Dark patterns are deliberate manipulation through the user interface..." [Kessler Page]

- **What You Can Do Today**
  - Use apps and timers to limit technology use.

- **Legislation / Bills**
  - S.2355 - End Racial and Religious Profiling Act of 2019

---

**Pract 1.9** Dark patterns

- **Implications for You**
  - Dark patterns are deliberate manipulation through the user interface.

- **Examples of Undesired Behavior**
  - Theophany has hired design experts out of the UC Berkeley School of Information.

- **Corresponding References**
  - "Dark patterns are deliberate manipulation through the user interface..." [Kessler Page]

- **What You Can Do Today**
  - Use apps and timers to limit technology use.

- **Legislation / Bills**
  - S.2355 - End Racial and Religious Profiling Act of 2019
<table>
<thead>
<tr>
<th>PRACTICE</th>
<th>DESCRIPTION OF DIGITAL IMPORT</th>
<th>IMPACTS FOR YOU</th>
<th>EXAMPLES OF UNDERECONOMIC BEHAVIOR</th>
<th>CORRIGENDA/REFERENCES</th>
<th>WHAT YOU CAN DO TODAY</th>
<th>IMMINENT ALLIANCE RECOMMENDATION</th>
<th>LEGISLATION/ILLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRP.5</td>
<td>Drawing a moral gray by translating an action into a “trending” by filing records, digital footprinting, and surveillance</td>
<td>Freedom of choice and movement is stifled based on judgement by machines</td>
<td>You are being manipulated and impacted in ways that are not in your interest.</td>
<td>[80]</td>
<td>Stay aware that use of your feedback into those systems and their interests to sway, in a headset, may be used in attempts by systems, actively as in a “Like” button, or passively such as an iris reading sensor.</td>
<td>S. 2763- Filter Bubble Transparency Act,    The Foreign Intelligence Authorization Act, S. 3456 Consumer Data Privacy and Security Act ,  H.R. 4978 Online Recognition Privacy Act ,  S.2355 - End Racial and Religious Profiling Act of 2019, S. 847 Commercial Facial Authentication Act (87], 2017</td>
<td></td>
</tr>
<tr>
<td>GRP.6</td>
<td>Digital identity services offer false hope to those who do not have reliable health and financial records, or are currently under employed or unemployed</td>
<td>Digital identity services offer false hope to those who do not have reliable health and financial records, or are currently under employed or unemployed</td>
<td></td>
<td>[80]</td>
<td>Stay aware that use of your feedback into those systems and their interests to sway, in a headset, may be used in attempts by systems, actively as in a “Like” button, or passively such as an iris reading sensor.</td>
<td>S. 2763- Filter Bubble Transparency Act,    The Foreign Intelligence Authorization Act, S. 3456 Consumer Data Privacy and Security Act ,  H.R. 4978 Online Recognition Privacy Act ,  S.2355 - End Racial and Religious Profiling Act of 2019, S. 847 Commercial Facial Authentication Act (87], 2017</td>
<td></td>
</tr>
<tr>
<td>GRP.7</td>
<td>AHIM.5 AI / Modeling / Computation [AIMC] Manipulation [MNIP] MNIP.1 AIMC.6 AIMC.5 MNIP.6 MNIP.3</td>
<td>Emotional manipulation</td>
<td>Emotional manipulation</td>
<td>[80]</td>
<td>Stay aware that use of your feedback into those systems and their interests to sway, in a headset, may be used in attempts by systems, actively as in a “Like” button, or passively such as an iris reading sensor.</td>
<td>S. 2763- Filter Bubble Transparency Act,    The Foreign Intelligence Authorization Act, S. 3456 Consumer Data Privacy and Security Act ,  H.R. 4978 Online Recognition Privacy Act ,  S.2355 - End Racial and Religious Profiling Act of 2019, S. 847 Commercial Facial Authentication Act (87], 2017</td>
<td></td>
</tr>
<tr>
<td>GRP.8</td>
<td>Overreach: The systems work by scanning resumes for contextual keywords and mathematically scoring them for relevance, and sending targeted ads to those leads.</td>
<td>Automated decision-making:  What if there is a failure in the systems and the research is either unconscious or not done in a systematic manner?</td>
<td>If an employer gains access to your DNA information, they could use it to manipulate you.</td>
<td>[80]</td>
<td>Stay aware that use of your feedback into those systems and their interests to sway, in a headset, may be used in attempts by systems, actively as in a “Like” button, or passively such as an iris reading sensor.</td>
<td>S. 2763- Filter Bubble Transparency Act,    The Foreign Intelligence Authorization Act, S. 3456 Consumer Data Privacy and Security Act ,  H.R. 4978 Online Recognition Privacy Act ,  S.2355 - End Racial and Religious Profiling Act of 2019, S. 847 Commercial Facial Authentication Act (87], 2017</td>
<td></td>
</tr>
</tbody>
</table>