Digital Harms Dictionary
Produced by Internet Safety Labs

PRACTICE	ID	DESCRIPTION OF DIGITAL HARM	IMPLICATIONS FOR YOU	EXAMPLES OF UNDESIRED BEHAVIOR	CORROBORATING REFERENCES	WHAT YOU CAN DO TODAY	ME2B ALLIANCE RECOMMENDATION FOR VENDORS	LEGISLATION / BILLS
Information Collection Practices [ICP]	ICP.1	Collecting information from the individual while interacting with the Service Provider's software without individual's consent.	Systems are collecting personal facts and details without permission. This can be aggregated with other information to build a model of you, your personality, your habits, etc.	Google tracking your search details and sharing with advertisers to display ads. Voice based personal assistants using spoken words to inform ads. Sensors performing passive data collection.	Amazon says its facial recognition can now identify fear https://www.cnbc.com/2019/08/14/amazon-says-its-facial-recognition-can-now-identify-fear.html ([7], 2019)	Opt out where possible. Read Terms of Service and Privacy Policy. Use Duck Duck Go instead of Google as a search engine.	Default initial state is no information collection allowed until formal relationship established and Agreement is [Relationship Terms are] established.	S.1822 - Broadband DATA Act, H.R.4978 - Online Privacy Act of 2019, S.3456 - Consumer Data Privacy and Security Act of 2020, S.1214 - Privacy Bill of Rights Act
	ICP.2	Collecting information about the individual and their behavior as they interact with the Service Provider's software, without individual's consent.	Systems are collecting personal behavioral information without your consent. In this instance, the Service Provider may offer information about what they are collecting, but they haven't satisfied the condition of obtaining consent. This is an invasion of privacy, no different from a smart speaker eavesdropping on all of your conversations. This kind of behavioral information can be aggregated with other information to build a model of you, your personality, your habits, etc. Algorithms and/or individuals may act on these factors and impact other areas of life unwelcome by the person(s) impacted. Often, these models are used to predict your behavior and manipulate you to make a purchase or take some action that is in the Service Provider's interest/to the Service Provider's benefit.	"Bundled into VR headsets or AR glasses, eye-tracking will, in the near-future, enable companies to collect your intimate and unconscious responses to real-world cues and those they design. Those insights can be used entirely for your benefit. But they will also be seen as priceless inputs for ad-driven businesses, which will learn, model, predict and manipulate your behavior far beyond anything we've seen to date." ([89], 2019) VR/AR headsets collecting information from iris regarding anxiety, relaxation, fear, etc.	https://www.vice.com/en_us/article/bj9gyv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail ([89], 2019)	Opt out where possible. Read Terms of Service and Privacy Policy. Use Duck Duck Go instead of Google as a search engine.	Default initial state is no information collection allowed until formal relationship established and Agreement is [Relationship Terms are] established.	S.3850 - Equitable Data Collection and Disclosure on COVID-19 Act, S.2398 Voter Privacy Act of 2019, H.R.8749 DATA Privacy Act, S.4626 SAFE DATA Act , H.R. 4978Online Privacy Act of 2019 Voter Privacy Act of 2019, H.R. 2013Information Transparency and Personal Data Control Act , S.1214 - Privacy Bill of Rights Act
	ICP.2a	Collecting information without the individual's awareness.	To differentiate from ICP.2, this harm is when the Service Provider fails to divulge what kinds of information is being collected. (Note that there is also no consent in this case.)	Vendor's app scans devices system libraries and uploads them to their server--ostensibly for app optimization, but there's no opt out and it's not disclosed. "Facebook scans system libraries from their Android app user's phone in the background and uploads them to their server This is called "Global Library Collector" at Facebook, known as "GLC" in app's code It periodically uploads metadata of system libraries to the server" Jane Manchun Wong @wongmjane ([8], 2019)	https://twitter.com/wongmjane/status/1167463054709334017 ([8], 2019)	Stay aware of the apps who do this.	Any information harvested from the Individual's device must be permitted by the individual through some form of valid consent.	H.R.4978 - Online Privacy Act of 2019, H.R.2610 - Fraud and Scam Reduction Act, S.4499 - COVID-19 Misinformation and Disinformation Task Force Act of 2020, S.1108 - Algorithmic Accountability Act of 2019, S. 3861 Exposure Notification Privacy Act , H.R. 2013Information Transparency and Personal Data Control Act , S.1214 - Privacy Bill of Rights Act
	ICP.3	Individual's consent or permission for data use was Defective. Meaning, that even though the individual may have performed a "consent action" (and there is recorded manifestation of consent), it fails to meet either the Autonomy condition (the individual wasn't coerced in some way to agree to something), or the Knowledge condition (the individual is provided with complete and clear information about what they are giving and how it will be used).	Often, we click Consent buttons that are presented to us online without really understanding what we're consenting to; this situation is called Defective Consent because the individual doesn't truly understand what's being collected or how it's used. Or sometimes, we are required to Consent to data collection in order to receive product upgrades and uphold product warranties. Since we want product warranties, we will consent even though we'd rather not share information; this situation is also Defective Consent, as it fails the condition of an individual acting with real autonomy. Both of these scenarios are harmful in that they give the illusion of control by giving the individual a Consent button, but they fail to meet the legal requirements for true consent.	Clickwrap TOS/TOU contracts.				S. 3861 Exposure Notification Privacy Act , H.R. 4978Online Privacy Act of 2019 , H.R. 2013Information Transparency and Personal Data Control Act
	ICP.4	Titles like Mr. Mrs. Miss -- Collecting unnecessary information.	Users may not wish to disclose their marital status or even associate their 'identity' with such a status. This is also a use of identity that brings societal sexist hierarchies into the technology space therefore giving them weight. This could have negative connotations and smacks of profiling. This is an example of data overreach: the Service Provider is collecting information that isn't strictly necessary to provide the expected service.	Many sites include titles and honorifics in name fields. A recent transaction with Costco Travel required the customer to provide both gender and title in order to book a trip.	Honorific, gender instead of sex under certain circumstances too (e.g I do NOT have a gender but I am female -I have been mandated to answer a 'what gender' question which did not have a 'no preference' option) https://www.bloomberg.com/news/articles/2019-11-09/viral-tweet-about-apple-card-leads-to-probe-into-goldman-sachs ([9], 2019)	Don't respond to these fields.	If used at all, these fields must be optional unless legally required.	S.2889-National Security and Personal Data Protection Act of 2019, H.R.6004 - Transparency and Accountability in Health Care Costs and Prices Act of 2020, S. 3861 Exposure Notification Privacy Act
	ICP.5	Marital Status -- Collecting unnecessary information.	As above marital status, unless it has a very specific requirement needed for a service to run, should not be a required data collection. Societal placement identifiers such as this, are often used to create hierarchies.	Examples of banks and similar authorities who will choose to send a communication to the husband as society still sees this as the 'head of household'. Divorced or separated spouses (particularly women) being unable to separate finances, as still seen as an appendage of their husband. Even in "real life", we are constantly confronted with paper forms that include marital status boxes that include "Divorced"--which has no bearing on nearly all services, where "Single" is sufficient, if needed at all.	Communications which are sent to the husband on behalf of the wife. My daughter had a row with a bank who always wrote to her partner and not her, assuming he was head of the household.	Don't respond to these fields.	If used at all, these fields must be optional unless legally required.	S.2355 - End Racial and Religious Profiling Act of 2019, S.2889-National Security and Personal Data Protection Act of 2019, H.R.6004 - Transparency and Accountability in Health Care Costs and Prices Act of 2020, S. 3861 Exposure Notification Privacy Act , H.R. 4978Online Privacy Act of 2019
	ICP.6	Gender -- Collecting unnecessary information.	Gender is a political hot topic in 2019. It is seen by some as being used to degrade sex-based rights. Also there are implications around gender bias.	Facebook - Gender only and choices male/female/custom. GMail is the same as above, has 'prefer not to say' - all gender collection, pointless, over collection of data for profiling. Even choosing 'prefer not to say' allows profiling - this just needs to be removed.	Recently, I was asked to complete a form for executives on IT initiatives. There was a gender box, with male/female/non-binary. There was no way to choose my sex and that I do not have a gender - gender is a social construct and can be damaging to women's biological sex-based rights. https://www.bloomberg.com/news/articles/2019-11-09/viral-tweet-about-apple-card-leads-to-probe-into-goldman-sachs ([9], 2019)	Don't respond to these fields.	Do not ask for sex or gender unless the service requires it to operate. For example, in healthcare, the sex would need to be known for certain reasons such as statistical analysis and medical interventions. Or at least allow a choice to not pick anything (non-mandatory where appropriate)	H.R.4978 - Online Privacy Act of 2019, S.2355 - End Racial and Religious Profiling Act of 2019, S.2889-National Security and Personal Data Protection Act of 2019, H.R.6004 - Transparency and Accountability in Health Care Costs an, S. 3861 Exposure Notification Privacy Act
	ICP.7	Service collects data that isn't necessary for the service. (e.g. Personalization at Scale using Data Management Platforms that aggregate first, second, and third party data allowing businesses a holistic picture of the individual. See LiveRamp by Axciom as an example.)	Additional profiling data made available to brokers, advertisers, etc. Negative correlations may develop whereas insurance rates may go up because the person's social connections may have "bad" driving records. The negative "scoring" of your associations become a shared liability and manifests i higher risk rates. Algorithms often use the "birds of a feather flock together" logic for this kind of grouping. While it may have some reasonable truth, it is not accurate in many cases.	from article: "Put simply, companies like LiveRamp and competitor Datalogix match offline databases to online data, often making the connection by using registration information gathered by travel, dating or news sites, or gaming system partners." ([10], 2014)	ACXIOM ACQUIRES LIVERAMP TO BOOST OFFLINE-TO-ONLINE DATA CAPABILITY https://adage.com/article/datadriven-marketing/acxiom-buys-liveramp-offline-online-data-capability/293212 ([10], 2014)	Write your congress people, connect with organizations like the Me2B Alliance to learn more.	Build your own relationships and profiles with your customers using information that they give you directly. Don't use data brokers.	S.2746 - Law Enforcement Suicide Data Collection Act, S.3850 - Equitable Data Collection and Disclosure on COVID-19 Act,. H.R.7689 -Improving Data Collection for Adverse Childhood Experiences Act, S.1108 - Algorithmic Accountability Act of 2019, S. 3861 Exposure Notification Privacy Act
	ICP.8	"Invisible" AI training data collection.	You are forceably made to help train computer vision every time you use reCaptcha at a website.	Many websites use reCAPTCHA ostensibly to ensure that their services aren't being leveraged by software bots, but really, the reCAPTCHA tasks are AI training data.	https://aibusiness.com/recaptcha-trains-google-robots/ ([11])	Recognize the trend and its implications and act and/or express yourself accordingly.	?	S.2943 - National Defense Authorization Act for Fiscal Year 2017*, S.4400 -National Biometric Information Privacy Act of 2020
Information Use Practices [IUP]	IUP.1	Personal Information is used by the Service provider beyond the user-permitted or legal usage. Note that this covers both the case where the individual enters the information, or the system passively collects behavioral information.	You have expectations and/or grant explicit permissions about how your personal information is to be used and the Service Provider exceeds those designated uses. For example, you may be shopping for a gift for your niece and you instruct the service to use the information during this shopping transaction only and not to be make suppositions about your personal preferences based on your shopping habits today. When you start seeing advertisements for teenage girl products in the retailer's app/website, you know that your preferences have been breached.	Brand/Retailer is allowing data brokers and ad-tech companies to track individuals on the brand/retailer's website and beyond	Here are the data brokers quietly buying and selling your personal information https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information ([1], 2019)	Use browsers that block such technology (e.g. BRAVE)	When a Me2B relationship is in place, permission must be provided/obtained by the individual for use of information. When a Me2B relationship isn't in place, the individual must be regarded as anonymous and their anonymity must be preserved.	S.4626- SAFE DATA Act, H.R.748 - CARES Act, H.R.7302 - Accessible, Affordable Internet for All Act,
	IUP.2	Personal Information is used by "third parties / Data Processors" beyond the user-permitted or legal usage (including behavioral data).	In this scenario, you have designated that your personal information may only be shared with 3rd parties for the purpose of providing the expected service. In the prior shopping example, for instance, you have set your preferences to not allow your information to be shared with 3rd parties only to fulfill the purchase transaction. You've selected a product from a 3rd party vendor. You know your preferences have been breached when you get subscribed to the 3rd party vendor's maillist, which is not a requirement to fulfill the transaction. The 3rd party/Data Processor is at fault in this breach.					H.R.2013 -Information Transparency & Personal Data Control Act, S.3456-Consumer Data Privacy and Security Act of 2020, S.2398 - Voter Privacy Act of 2019, S.1214 -Privacy Bill of Rights Act, H.R.6675 - Data Broker Accountability and Transparency Act of 2020, S.2577 - Data Broker Accountability and Transparency Act of 2019S. 3861 Exposure Notification Privacy Act , S. 3456Consumer Data Privacy and Security Act
Information Sharing Practices [ISP]	ISP.1	Sharing individual's information with other Service Providers or Individuals, other than those permitted--or reasonably expected--by the Individual/Data Subject.	This is similar to IUP.2, but in this case, the Service Provider is responsible for breaching your preferences. In the shopping example above, you have configured your setting to disallow sharing your information with any 3rd parties other than those involved in the transaction. You know this is breached when you start seeing ads in your browser for teen age girl products.	1 - Food consumption information (grocery purchases, restaurant visits) provided to a loyalty program is used to determine healthcare premiums for the individual. 2 - Recruiters can use software to analyze a candidate's social media behavior and environment (friends, tone of voice, opinions) to determine if the candidate gets even invited for an interview. 3 - Consumer DNA sites such as 23andMe and Ancestry using data for research 4 - Facebook allows 3rd party use of my photo to advertise something without my consent. Thus images of a person may be associated with people, products and services they may not approve of. 5- Sleep Number T&C: "We do not guarantee that data submitted or transmitted to Us will be free from unauthorized disclosure, access, misappropriation, or intrusion."	2 - Keep It Clean: Social Media Screenings Gain in Popularity https://www.businessnewsdaily.com/2377-social-media-hiring.html ([2], 2018) 3 - How DNA Companies Like Ancestry And 23andMe Are Using Your Genetic Data https://www.forbes.com/sites/nicolemartin1/2018/12/05/how-dna-companies-like-ancestry-and-23andme-are-using-your-genetic-data/#520215e56189 ([3], 2018) 4- https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/unauthorized-transmission-and-use-of-personal-data/ ([4], 2012) 5 - https://www.sleepnumber.com/sleepiq-end-user-agreement ([5])	1 - Look carefully into loyalty programs. Assume that your purchase behavior is being tracked and shared. Use TOS;DR. 3 - Do not donate DNA samples to non-HIPPA compliant services. 4. 1. Adjust advertisement sharing if offered. 4.2 Do not join services which allow your personal data artifacts to be handed out to other parties. 5. Disable "Smart" system automation features, and control communications manually; do not purchase "connected" / IoT products, or disable WiFi capability.	When a Me2B Relationship is in place, it must be strictly adhered to. The individual drives the terms of the Me2B Relationship.	H.R.2013 -Information Transparency & Personal Data Control Act, S.3456-Consumer Data Privacy and Security Act of 2020, S.2398 - Voter Privacy Act of 2019, S.1214 -Privacy Bill of Rights Act, H.R.6675 - Data Broker Accountability and Transparency Act of 2020, S.2577 - Data Broker Accountability and Transparency Act of 2019, Misuse of voluntarily shared information, S. 3456Consumer Data Privacy and Security Act

PRACTICE	ID	DESCRIPTION OF DIGITAL HARM	IMPLICATIONS FOR YOU	EXAMPLES OF UNDESIRED BEHAVIOR	CORROBORATING REFERENCES	WHAT YOU CAN DO TODAY	ME2B ALLIANCE RECOMMENDATION FOR VENDORS	LEGISLATION / BILLS
	ISP.2	Misuse of voluntarily shared information with peers in social media platforms or other platforms	The challenge of "public privacy" is in play here. As people are different, there will be differing senses of appropriate boundaries and what is "private".	Posting something in a limited exposure space (Only Friends See) and having that lifted out into an open space (Everyone Sees) by a "Friend" who has access to the info in a bounded space. "Photos and videos posted to private accounts on Instagram and Facebook aren't as private as they might seem. They can be accessed, downloaded, and distributed publicly by friends and followers via a stupidly simple work-around. The hack — which works on Instagram stories as well — requires only a rudimentary understanding of HTML and a browser. It can be done in a handful of clicks. A user simply inspects the images and videos that are being loaded on the page and then pulls out the source URL. This public URL can then be shared with people who are not logged in to Instagram or do not follow that private user." ([6], 2019)	https://www.buzzfeednews.com/article/ryanhatesthis/private-instagram-posts-arent-exactly-private ([6], 2019)	Use permissions when sharing on social networks to prevent forward-sharing, when possible. Be mindful about what you're sharing, and what your permissions are for each item you post.	Vendor should allow user to create permissions including "download y/n". Vendors/Platforms illuminate privacy consideration to visiting users by popping up a message suggesting image may be marked private. Vendors/Platforms do not facilitate direct "Save As" or copy of images and/or text from private data spaces	H.R.2013 -Information Transparency & Personal Data Control Act, S.3456-Consumer Data Privacy and Security Act of 2020, S.2398 - Voter Privacy Act of 2019, S.1214 -Privacy Bill of Rights Act, H.R.6675 - Data Broker Accountability and Transparency Act of 2020, S.2577 - Data Broker Accountability and Transparency Act of 2019, Misuse of voluntarily shared information, S.2186 - Protecting Personal Information Act of 2019
Inverse Privacy / Data Brokers [IPDB]	IPDB.1	Data brokers buy and sell information about Individuals, where said Individuals have no relationship with Data Brokers or ability to monitor, correct, or remove information.	Individual's information is being bought and sold without any opportunity for individual to consent, correct, or ask to be forgotten.	Examine any data broker, such as Acxiom, Nielsen, Experian, Equifax https://www.forbes.com/sites/bernardmarr/2017/09/07/where-can-you-buy-big-data-here-are-the-biggest-consumer-data-brokers/#65029d7e6c27 ([12], 2017) https://www.newsweek.com/secretive-world-selling-data-about-you-464789 ([13], 2016)	https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information ([14], 2019)	For now, be extremely wary of all free services.	Data brokers must accept content only from the Individual (Data Subject) directly. B2B "Gossip" channels are discouraged but can be allowed so long as the Individual consents to it directly with the Data Broker, which also results in the establishment of a Relationship between the Individual and the Data Broker.	S.2885 - Stop Marketing And Revealing The Wearables And Trackers Consumer Health Data Act, H.R.6321 - Financial Protections and Assistance for America's Consumers, States, Businesses, and Vulnerable Populations Act, S.2342 -Data Broker List Act of 2019, S.2186 -Protecting Personal Information Act of 2019
	IPDB.2	"...companies give assurances...that they do not sell their data to unaffiliated outsiders, but it is still available to their advertising "partners." ([4], 2012)	"...gives the companies, not to mention the subjects of the data, even less control over where it goes and how it is used." "Marketers have an immense appetite for personal information too. They use collective data, along with sophisticated statistical analysis techniques and psychological models, to predict peoples' purchasing preferences and behavior and to identify those factors that most strongly influence consumers' loyalty and choices. 6 They then combine this intelligence with detailed information on specific individuals and subgroups of consumers to try to engage them and influence their buying decisions. Not only do they want contact information, such as names, addresses, phone numbers, email addresses and net IDs, but also more personal information, such as shopping habits, amount of assets, type of car owned, family situation, age, gender, and so on, to target and adapt their advertising. This information can be purchased from credit agencies, motor vehicle departments, the post office and many other sources, as well as gleaned from public records. It can also be generated internally. Supermarkets, department stores and other retailers can now keep track of the items purchased by each customer, both online and in-store, and, if the customer uses a credit card, bank card or store identification, can link the purchases with the customer's name and address, age, gender and other characteristics. But the richest and most lucrative source of information, as well as direct contact with consumers, is through information portals like Google and social networks, particularly Facebook. This information can be used to personalize ads according to the characteristics, circumstances and preferences of each individual, especially when the ads are delivered directly online. Now, with the development of mobile apps that track a	1 - "Most users have no awareness that their personal thoughts, interests and habits are so exposed." ([4], 2012) 2 - "...it can be commandeered by government bodies for use in surveillance, investigations, and criminal and legal proceedings." ([4], 2012)	https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/unauthorized-transmission-and-use-of-personal-data/ ([4], 2012)	Use cash when possible. Choose "card" and vendor relationships who demonstrate preferred terms and conditions regarding your values.	Don't build a business solely on data aggregation and monetization such as data brokers.	S.2943 - National Defense Authorization Act for Fiscal Year 2017, H.R.2013 - Information Transparency & Personal Data Control Act, S.2342- Data Broker List Act of 2019, S.2186-Protecting Personal Information Act of 2019, H.R.2013 - Information Transparency & Personal Data Control Act, S.1214 - Privacy Bill of Rights Act
Supplier Lock-in & Contracts of Adhesion [LICA]	LICA.1	Forcing people to agree to Terms of Service and Privacy Policy in order to use a product or service they may have already paid for. (contracts of adhesion)	We're constantly forced into accepting TOS and privacy policies during hardware and software configuration, though we never read them. (And even if we did, we can't understand exactly what service providers are doing, and even if we could do that, there's no way for us to audit or monitor the company's behavior to ensure they're doing what they promised.)	Virtually every connected product and service requires agreement by the end user to the TOS and Privacy Policy.		Use TOS;DR	Make your TOS and Privacy Policies short and understandable. Ultimately, evolve your IT backend to accept user-proffered Right to Use Licenses and Terms.	H.R.4978 - Online Privacy Act of 2019, H.R.4978 - Online Privacy Act of 2019, S.4626 - SAFE DATA Act , H.R.2013 - Information Transparency & Personal Data Control Act, S.1214 - Privacy Bill of Rights Act
	LICA.2	Forcing people to agree to usage surveillance in order to receive software upgrades, warranty service, and high quality experience over time. (contracts of adhesion)	Loss of autonomy and agency. Victim of coercion.	"The Windows 10 default privacy settings leave a lot to be desired when it comes to protecting you and your private information." [85]	https://pixelprivacy.com/resources/windows-privacy-settings/ ([85], 2019)	Carefully review setup options during installation of software and devices. Using the "Custom Set Up" usually offers granular selection of these options.		H.R.4978 - Online Privacy Act of 2019, H.R.4978 - Online Privacy Act of 2019, S.1214 - Privacy Bill of Rights Act
	LICA.3	Disallowing people to modify hardware and software configurations for purchased hardware and software.	A range of decisions concerning a "free and clear purchased hardware and software" does not exist without a form of penalty. Acting outside of certain bounds is penalized actively or passively, it is not supported and seen as a hack from Apple's perspective.	The Lock-In is positioned as a protective "feature" of iOS. Apple states "unauthorized modification of iOS is a violation of the iOS end-user software license agreement and because of this, Apple may deny service for an iPhone, iPad, or iPod touch that has installed any unauthorized software"	https://support.apple.com/en-us/HT201954 ([15], 2018)	Value judgement: Is it worth losing warranty for freedom?		H.R.4978 - Online Privacy Act of 2019, S.1214 - Privacy Bill of Rights Act
Identity Practices [IDPR]	IDPR.1	No easy, trusted way for people to authenticate the identity of the Service Provider in using websites or apps.	The browser lock icon was a start, but they and certs have been spoofed.	A. "In current ongoing scams, criminals are sending phishing emails pretending to be from an acquaintance or official website. But links in the emails actually go to malicious sites, masquerading as legitimate services using HTTPS as cover."	A. https://www.nextgov.com/cybersecurity/2019/06/fbi-warning-lock-icon-doesnt-mean-website-safe/157629/ ([16], 2019) B. https://www.ic3.gov/media/2019/190610.aspx ([17], 2019)	B. "The FBI offered four tips to avoid becoming a victim: 1. Do not simply trust the name on an email: question the intent of the email content. 2. If you receive a suspicious email with a link from a known contact, confirm the email is legitimate by calling or emailing the contact; do not reply directly to a suspicious email. 3. Check for misspellings or wrong domains within a link (e.g., if an address that should end in ".gov" ends in ".com" instead). 4. Do not trust a website just because it has a lock icon or "https" in the browser address bar."	SSI for vendors. "MyVendor Validator" agent.	H.R.4978 - Online Privacy Act of 2019, S.1214 - Privacy Bill of Rights Act
	IDPR.2	Loss or Misuse of acquired Finger Print scan data	Unique, physical biometric data may now become part of the digital data stream	Improper care of data and storage of biometrics. For example, not storing biometric as a hash	https://tech.newstatesman.com/security/fingerprints-biometric-security ([18], 2019)	Use proper security, including hash functions, robust authentication, correct configuration of databases, etc. This will include good design of the overall system using biometrics to ensure that security is by design		S. 4400National Biometric Information Privacy Act of 2020
	IDPR.3	Loss or Misuse of acquired Facial Recognition scan data	Unique, physical biometric data may now become part of the digital data stream	Improper care of data and storage of biometrics. For example, not storing biometric as a hash.	https://www.theverge.com/2019/8/8/20792326/facebook-facial-recognition-appeals-decision-damages-payment-court ([19], 2019)	Dependent on the vendor having robust security measures. Avoid vendors with poor security record.	Use proper security, including hash functions, robust authentication, correct configuration of databases, etc. This will include good design of the overall system using biometrics to ensure that security is by design. Sharing biometric data for diagnostic or performance improvement purposes should be opt-in, with data anonymized and made as audit-able as possible. People should have their own forms of facial recognition, for example to unlock phones or to sort through old photos. But, the data they gather should not be shared with the company providing the facial recognition software (unless it's just of their own face, and then only for the safest possible diagnostic or service improvement purposes).	S. 847 Commercial Facial Recognition Privacy Act , S. 4400National Biometric Information Privacy Act of 2020
	IDPR.4	Relying parties requesting data they don't need (this is above and beyond data minimization arguments) ? - Is "Creation of Unnecessary Data/Privacy Risk" reasonable as a descriptor of this harm?	Users may not wish to disclose their marital status or even associate their 'identity' with such a status. This is also a use of identity that brings societal sexist hierarchies into the technology space therefore giving them weight. This could have negative connotations and smacks of profiling	I have been mandated to answer a 'what gender' question which did not have a 'no preference' option. Honorific, gender instead of sex under certain circumstances too (e.g I do NOT have a gender but I am female)	No specific articles on this (maybe I should write one?) Vast majority of online accounts will request an honorific, however.	If not a mandated field, chose not to give your honorific. However, many registration processes mandate the use of an honorific. Similarly for other fields that you feel uncomfortable answering, such as gender/age/political queries, and so on.	Do not ask for sex or gender unless the service requires it to operate. For example, in healthcare, the sex would need to be known for certain reasons such as statistical analysis and medical interventions.	S. 3861 Exposure Notification Privacy Act "
	IDPR.5	Universal IDs	"...a centralized database can be used to track anyone's physical movements and private life, thus infringing on personal freedom and privacy... The management of disparate linked systems across a range of institutions and any number of personnel is alleged to be a security disaster in the making."	Browser based Universal anonymous ID: " IAB-led effort to create a standardized online user ID that's designed to reduce the online ad industry's reliance on third-party cookies. DigiTrust, a non-profit acquired by the IAB Tech Lab last year, is working to create a universal, persistent and anonymized	https://en.wikipedia.org/wiki/Identity_document ([83])	If not mandated, you need not apply for this type of ID.		

PRACTICE	ID	DESCRIPTION OF DIGITAL HARM	IMPLICATIONS FOR YOU	EXAMPLES OF UNDESIRED BEHAVIOR	CORROBORATING REFERENCES	WHAT YOU CAN DO TODAY	ME2B ALLIANCE RECOMMENDATION FOR VENDORS	LEGISLATION / BILLS
Inadequate Managing End of Account/End of Life [EOLA]	EOLA.1	No way to delete an account; User can deactivate account, but Vendor doesn't delete account and all information; no easy way to delete all information.	Removes ability to have control once account created.	Sleep Number Bed T&C: "We also collect, store, and use Third Party Data when You choose to interface with Third Party Services. We store Your Data and the Third Party Data in Our databases and servers, and may continue to store such data after You cancel or deactivate the Services and/or Your User Account(s)." It isn't just about deleting an account, it is about an easy way to do so, for example: xtensio - document creation portal, you have to go through a contact process to have your account and data deleted. Services also may not delete data, but only deactivate an account.	https://www.sleepnumber.com/sleepiq-end-user-agreement ([5])	Delete account and associated data (securely) mandatory) - note there may be some laws that prevent full data deletion for a given amount of time (government identity services included - they day its for 'audit' purposes)	Always offer a close/delete account option. This can have rules associated that give a 'cooling off' period to prevent change of mind. Make this option obvious and not hidden.	S. 3861 Exposure Notification Privacy Act,
	EOLA.2	Death of account holder leads to account takeover	Fraud and general upset for family and friends when a dead person suddenly tries to connect to them	Email, Skype accounts unable to be easily closed by family members. This leaves them open to account takeover.	Multitude of examples, Skype for example, it is difficult to close an account after a person has died. Family members have to go through a process to do so - this will be for security reasons, but a better system should be offered.	When a loved one dies you will have to currently defer to the process that may be in place with the service. Not all services offer this and account handover is not possible	Proper ways to deal with digital death, including account delegation (techno-legal solutions)	
	EOLA.3	I want to not just "unsubscribe" I want to --with one button--"Forget Me" Related to EOLA.1, but it's when the Me2B Relationship is just a "Marketing Subscription".	Relationships which are no longer timely or valued and not be easily terminated. Thereafter the ongoing connection causes "noise" but no value. Also, many of us have experienced the continuation of receiving marketing email even after unsubscribing, perhaps more than once.	A. "Verizon has a page about cancelling service, but people don't like it much. The average rating of 1000 users is one out of five stars."	A. https://unbounce.com/conversion-rate-optimization/when-friction-is-good/ ([20], 2016)	Use a service like Unroll.me to help reduce marketing noise, though this doesn't solve the problem.	Don't force premature Me2B Relationships. Let individuals be in charge of the relationship; let them indicate when they want to provide an email address.	S.1214 - Privacy Bill of Rights Act
Security Practices [SP]	SP.1	Poor phishing practises	Hard to differentiate a real brand email from a phishing email	Not using the name of a customer in the salutation Having a clickable link in an email (should use advise such as losing to your account or similar)	Sending emails with links to important actions, such as account updates, etc. Not applying the advisories of orgs like APWG	Send emails from main, recognizable domain; direct users to make sensitive account changes from their site (without linking); document communication practices in their support center Avoid using links in emails	Offer security awareness around phishing for your customer base (e.g. videos, etc.) Use DMARC guidance on phishing.	S.4626 - SAFE DATA Act, S. 3861 Exposure Notification Privacy Act , H.R.2013 - Information Transparency & Personal Data Control Act
	SP.2	Lack of support for 2FA (Two Factor Authentication) or MFA (Multi-factor Authentication) to control account access	Credential stuffing and account take over attacks are easier to conduct w/o 2FA and or MFA. On the flip side, it creates high friction when changing devices, phone numbers, and forgetting your password	23andme only use first factor but the data it holds is highly sensitive Some Credit file agencies (CreditKarma in the UK) only use first factor but have highly sensitive information available online	See 23andme and https://www.creditkarma.co.uk/ account creation process	If the service offers you the option to setup a second factor, do so. However, not all services offer this option. To reduce your threat of an account being hacked or taken over, make sure you are careful about any emails that contain links or attachments (they could be phishing emails) and make sure any passwords you do use are not shared, unique to each account, and robust (see advice here: https://www.getsafeonline.org/protecting-yourself/passwords/ _)	Offer or require 2FA/MFA during account setup and make a concerted effort for feature adoption for users that signed up before the requirement Implement 2FA for accounts that hold personal and sensitive data.	S.4626 - SAFE DATA Act, S. 3861 Exposure Notification Privacy Act , H.R.2013 - Information Transparency & Personal Data Control Act
	SP.3	Only offers SMS/Text MFA	While SMS is better than nothing for most consumers, it leaves them vulnerable to SIM hijacking takeovers; That being said, it also increases the friction when the user is locked out of their account by forgetting their password or losing / replacing their device that manages their OTP (One Time Password) application	Any recovery system that does not offer recovery paths other than local device based text notification.	https://www.symantec.com/connect/blogs/password-recovery-scam-tricks-users-handing-over-email-account-access ([86] 2015)	Duo, Google authenticator app, and others are great vendors in this OTP MFA space	Offer OTP MFA	S. 3861 Exposure Notification Privacy Act
	SP.4	Creating a false sense of security	It is very difficult for people to know what is real and what isn't. Vendors need to come up with more elegant solutions to consumer security sense	58% of phishing sites use HTTPS: https://docs.apwg.org/reports/apwg_trends_report_q4_2018.pdf ([21], 2019)	Google has mandated the use of HTTPS by all - penalizing them with poor search results otherwise. Whilst on the surface this may seem sensible, in reality this has not worked. Now more than 50% of spoof sites are HTTPS (see APWG reports).	Be aware that not all sites with HTTPS are secure - be phishing aware.	Offer security awareness around phishing for your customer base (e.g. videos, etc.) Use DMARC guidance on phishing.	S. 3861 Exposure Notification Privacy Act
	SP.5	No phone / email verification	Makes it easy for account takeover with password resets	Any website or app that doesn't verify using phone or email.		Be wary of sites/services that don't require verification during account set up.	Require verification to complete the signup process	S.4626 - SAFE DATA Act
	SP.6	Primative Password Strength Feedback	Password strength validation relies only on validation of mixed character sets allowing users to reuse similar, potentially previously compromised, passwords across most services making them vulnerable to credential reuse and credential stuffing attacks.	Multitude all over the internet	https://haveibeenpwned.com/	Passwords should be compared against databases of known compromised passwords and not mark previously compromised passwords as "Strong"		S. 3861 Exposure Notification Privacy Act
IRL Hybrid Practices [IRLH]	IRLH.1	Online store sells sells harmful, banned and counterfeit products.	1. Value of the exchange is below the cost. Holder may unknowingly be liable for possession of legally toxic products. 2. A product marked with a credible mark of assurance is not actually qualified as "Safe".	1. A buyer unwittingly acquires a counterfeit item. It is sold thereafter resold to another buyer who determines the in-authenticity and takes legal recourse vs unwitting buyer of the counterfeit item. 2. "In 2016, UL partnered with Apple to evaluate the dangers of counterfeit iPhone chargers. In a controlled test program, our engineers tested 400 counterfeit adapters bearing UL marks and the results were literally shocking: the overall failure rate exceeded 99 percent. All but three adapters presented fire and shock hazards. Twelve were so poorly made that they posed a risk of electrocution."	1. "Tiffany & Company was spending millions of dollars chasing down counterfeit jewelry and other items on the Internet. Large groups of offenders were listing counterfeit Tiffany items on eBay. Therefore, Tiffany decided to sue eBay for trademark infringement claiming that the online auction house facilitated the sale of the counterfeit items. The Federal District Court in Manhattan disagreed with Tiffany on all counts and in April of this year the Second Circuit Court of Appeals agreed." https://www.practicalecommerce.com/Legal-When-Merchants-Are-Liable-for-Selling-Counterfeit-Brands ([22], 2010) 2. https://www.finance.senate.gov/imo/media/doc/35965.pdf ([23], 2018) 3. https://www.theverge.com/2019/8/23/20829933/amazon-selling-third-party-unsafe-banned-products-wsj-report ([24], 2019)	Be mindful and aware as an online shopper. Look for certifications such as UL, NSF, etc.		
	IRLH.2	Beacons in stores/retail active without consent, choice, and/or transparency.	Retail beacons track your presence and your behavior: how long you stay in a store, what parts of the store you spend more time in, etc. ostensibly to provide you with personalized location based deals and information. Services are uniquely identifying you and potentially correlating mass data, including behavior, and use it for whatever purpose they want. "Beacons and other sensors, however, can detect a phone's MAC address and register its location without any apps or even consumer knowledge...."It's only when you've opted into an app that I know it's you,'" "'The MAC address is a unique identifier," says the World Privacy Forum's Dixon. "It's very simple at this point to attach a MAC address with a unique user."	"Apple has been a leader in the field. Its iBeacon technology was built into its iOS7 operating system and lets iPhones and iPads constantly scan for nearby iBeacon transmitters. Once the device identifies an iBeacon sensor, it can wake up an app on the phone, even if that app is closed."	https://www.rightpoint.com/thought/2018/11/16/beacon-technology ([25], 2018) https://www.creditcards.com/credit-card-news/retailer-beacons-track-phone-shop-privacy-1280.php ([26], 2014)	1) Turn off Bluetooth [does this disable iPhones iBeacon?]. (2) only download retail apps for trusted vendors.	(1) Handset Manufacturers: default state is no beacon/transmitting. (2) Retailers: Need a new solution where beacon is controlled by downloaded application, which defaults to Beacon Disabled until user enables it. (3) offer individual easy methods to fine tune permissions beacons. (4) don't use MAC address to id individuals.	S.1108 - Algorithmic Accountability Act of 2019, S. 3861 Exposure Notification Privacy Act , S. 3456Consumer Data Privacy and Security Act
Burden of Decision-making [BODM]	BODM.1	The burden for ensuring a dignity- and privacy-respecting relationship is placed on the user.	People must have legal and technical know-how plus time and resources to fully study Terms of Service and Privacy policies for "every" service provider in their lives. And fine tune settings to reasonable privacy [for me]. Research in 2012 found it would take 76 working days to read all Privacy Policies alone. Implication to US national GDP: $781B annual cost.	Burying sensitive privacy settings in menus.	https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/ ([27], 2012)	Use TOSDR.org. Use privacy settings. Talk to your congresspeople.	Make readable, highly understandable and brief TOS and Privacy Policies.	
	BODM.2	"Consent and control quickly turn FIPs-based privacy rules into formalistic exercises designed to extract consent and use the gift of control to saddle the data subject with the risk of loss for data misuse."	In poorly constructed consent schemas, users bear the risk without any real agency. What seems like "control" isn't, but still puts the risks onto the individual.	Nearly all cookie consent User experiences. Clickwrap, Browsewrap, Scrollwrap and SignInWrap are all legally enforceable in the US, but reflect the harm of putting the burden of risk squarely on the individual.	https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3759&context=mlr ([28], 2017) https://proctorbrant.com/clickwrap-and-other-types-of-online-contracts-four-principles-to-follow-in-creating-a-legally-enforceable-electronic-agreement/ ([29], 2019)	Talk to your congresspeople.	Make readable, highly understandable and brief TOS and Privacy Policies.	
		SURV.1	Manufacturers fail to disclose recording capabilities in connected devices.	Microphones and cameras may record and share audio/visual data without knowledge or consent, disclosing confidential or sensitive information.	IoT or other connected hardware device unexpectedly and unknowingly has a microphone and or camera or other tracking sensor.	https://www.reuters.com/article/us-alphabet-nest/google-fails-to-disclose-microphone-in-nest-secure-idUSKCN1Q92FB ([30], 2019)	Carefully read product packaging, and hope it discloses all dormant capabilities.	All IoT and other hardware devices must clearly indicate if they have audio and/or visual recording capabilities, including who has access to the media files/streams. If so, the individual must grant permission to all uses.	S.1108 - Algorithmic Accountability Act of 2019
		SURV.2	Connected devices are always listening and possibly storing recordings.	Recorded media could be shared with third party services for monetization means unbeknownst to you. Recorded media could be shared with humans for additional natural language processing.	1. Through Siri, Apple contractors hear "countless instances of recordings featuring private discussions between doctors and patients, business deals, seemingly criminal dealings, sexual encounters and so on. These recordings are accompanied by user data showing location, contact details, and app data." 2. Amazon uses humans to parse commands and perform additional AI analysis. ("Mechanical Turk") 3. Smart TVs are watching you. " Vizio's Smart TVs track your viewing habits and share it with advertisers, who can then find you on your phone and other devices."	Siri https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings ([31], 2019) Amazon: https://www.cnn.com/2019/04/11/tech/amazon-alexa-listening/index.html ([32], 2019) Vizio: https://arstechnica.com/information-technology/2015/11/own-a-vizio-smart-tv-its-watching-you/ ([33], 2015)	Use video camera/webcam lens covers on all devices with cameras. Mute the microphone when not in use. Unplug device when not in use. Organizations who employ "Mechanical Turk"/ Human AI enhancement: use appropriate screening and security practices to staff Human AI team.	All hardware devices must include physical lens covers and mute buttons.	S.1108 - Algorithmic Accountability Act of 2019
		SURV.3	Connected devices collect [unexpectedly] sensitive information and may share for unexpected reasons.	Disclosure of minor to highly sensitive information can be unexpectedly used or hacked and abused.	Roombas have been busy mapping our homes, and now that data could be shared at any point in the future without our consent or awareness.	Roomba - https://www.theverge.com/2017/7/24/16021610/irobot-roomba-homa-map-data-sale ([34], 2017)	Read the Privacy Policy very carefully. Ask experts. Disable internet connectivity.	All devices must have an ability to disable the Internet-enabled "smart" capability.	S.1108 - Algorithmic Accountability Act of 2019, S. 3861 Exposure Notification Privacy Act
		SURV.4	Surveillance data is being shared externally beyond bounds agreed to by the individual.	Wide variety of surveillance possibilities. Information shared with state agencies can lead to unintentional Surveillance State activities.	Amazon Ring doorbells may be distributed by local law enforcement agencies thereby creating de facto surveillance environments.	Ring: https://www.usatoday.com/story/tech/2019/07/19/amazons-ring-doorbell-cameras-raise-fears-surveillance-police/1775707001/ ([35], 2019)	Express your opinion to local authorities related to this type of collaboration between personal devices and authorities. Do not contribute to apps that provide access to shared surveillance data.	TBD	H.R.4978 - Online Privacy Act of 2019

PRACTICE	ID	DESCRIPTION OF DIGITAL HARM	IMPLICATIONS FOR YOU	EXAMPLES OF UNDESIRED BEHAVIOR	CORROBORATING REFERENCES	WHAT YOU CAN DO TODAY	ME2B ALLIANCE RECOMMENDATION FOR VENDORS	LEGISLATION / BILLS
Surveillance [SURV]	SURV.5	Manufacturers don't allow individuals to disable recording capabilities in certain devices.	Devices are potentially always listening, watching and storing/sharing/using recorded information.	1."...even if you opt out, your voice commands will still be captured. The SmartTV has a set of pre-programmed commands that it recognizes even if you opt out of voice recognition. Samsung will collect the text of those pre-programmed voice commands (though not your voice itself) and analyze how much you're using certain command."	https://www.securityweek.com/when-iot-comes-office ([36], 2006) https://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/index.html ([37], 2015)	Use video camera/webcam lens covers on all devices with cameras. Mute the microphone when not in use. If can not Mute, unplug device when not in use.	All hardware devices must include physical lens covers and mute buttons. And/or provide software controls to selectively disable microphones, cameras, etc.	S. 3861 Exposure Notification Privacy Act
	SURV.6	Keyboards digital phenotyping.	As you use your device(s) patterns of use, such as number of keystrokes a minute, may be used to attempt to recognize your mood/emotional state.	Sharecare says it doesn't record the content of the calls it scans, it does collect phone numbers without informing the user.	https://medcitynews.com/2019/01/digital-phenotyping-a-revolution-or-a-privacy-breach/?rh=1 ([38], 2019)	Make certain that this data collection method is not a part of the terms and conditions for apps being considered for use. Use up to date security/scanning software to surface these exploits in case they have been delivered covertly.		S.1108 - Algorithmic Accountability Act of 2019,
	SURV.7	Key stroke Surveillance	Any information being typed may be captured for later use.	"...criminals use keyloggers. They scrape up passwords, credit card and banking information, personal details, and more, to use in identity theft and other malicious deeds."	https://www.pcworld.com/article/3199020/keyloggers-what-you-need-to-know-about-this-hidden-threat.html ([39], 2017)	Keep your virus protection up to date and active.		S.1108 - Algorithmic Accountability Act of 2019, S. 3861 Exposure Notification Privacy Act
	SURV.8	Surveillance is applied racially.	"...marketed as localized social networks where people in a neighborhood can discuss local issues or share concerns. But all too often, they facilitate reporting of so-called "suspicious" behavior that really amounts to racial profiling. Take, for example, the story of an African-American real estate agent who was stopped by police because neighbors thought it was "suspicious" for him to ring a doorbell." ([40], 2019)	"...African-American real estate agent who was stopped by police because neighbors thought it was 'suspicious' for him to ring a doorbell." ([40], 2019)	https://www.eff.org/deeplinks/2019/08/amazons-ring-perfect-storm-privacy-threats ([40], 2019)	Spread awareness and education to people of the risks involved. Societies need to continually address systemic racial and other bias.	Vendors need to continually be vigilant to how technologies can be used in harmful ways, including propagating bias.	S. 3861 Exposure Notification Privacy Act , S.2355 - End Racial and Religious Profiling Act of 2019,
	SURV.9	Zombie Cookies, Flash Cookies & Perma Cookies	"A zombie cookie is an HTTP cookie that is recreated after deletion. The term was created by Attorney Joseph H. Malley who initiated the Super-Cookie Class Actions in 2010. Cookies are recreated from backups stored outside the web browser's dedicated cookie storage. It may be stored online or directly onto the visitor's computer, in a breach of browser security. This makes them very difficult to remove. These cookies may be installed on a web browser that has opted to not receive cookies since they do not completely rely on traditional cookies." [wikipedia]	Flash Cookies [epic reference]	https://en.wikipedia.org/wiki/Zombie_cookie ([40]) https://epic.org/privacy/cookies/flash.html ([41], 2005)	https://www.reputationdefender.com/blog/privacy/how-to-delete-flash-cookies-permacookies-and-zombie-cookies ([42], 2018)	Don't use zombie cookies, flash cookies or perma-cookies. Minimize cookie usage in general.	S.1108 - Algorithmic Accountability Act of 2019, H.R.4978 - Online Privacy Act of 2019 , •The EU Cookie Directive
	SURV.10	Browser fingerprinting uniquely identifies individuals	"A device fingerprint, machine fingerprint, or browser fingerprint is information collected about a remote computing device for the purpose of identification. Fingerprints can be used to fully or partially identify individual users or devices even when persistent cookies (and also zombie cookies) can't be read or stored in the browser, the client IP address is hidden, and even if one switches to another browser on the same device.[1] This may allow a remote application to detect and prevent online identity theft and credit card fraud,[2][3] but also to compile long-term records of individuals' browsing histories even when they're attempting to avoid tracking, raising a major concern for internet privacy advocates." ([wikipedia])		https://pixelprivacy.com/resources/browser-fingerprinting/ ([43]) https://restoreprivacy.com/browser-fingerprinting/ ([44]) https://en.wikipedia.org/wiki/Device_fingerprint ([45])	Use privacy respecting browsers such as Brave, Firefox, Tor. Use the browser in "incognito mode" when possible. Use Panopticlick, Privacy Badger or other browser tools. To see your info use www.deviceinfo.me, and https://amiunique.org/ [restoreprivacy.com reference has excellent list of suggestions] Also here: https://amiunique.org/tools	Don't do this. Minimize cookie usage.	S.1108 - Algorithmic Accountability Act of 2019, S. 4400National Biometric Information Privacy Act of 2020
	SURV.11	Canvas Fingerprinting	"Canvas fingerprinting actually recognizes your browser of choice based on its configuration. Information about the browser, operating system, fonts and other pieces of data are combined to create a unique profile. Once the profile is built, it can be shared with other sites and ad networks. In other words, you can be tracked without using cookies." [EPICxx]		https://www.engadget.com/2018/06/05/apple-safari-canvas-fingerprinting/ ([46], 2018)	Use privacy respecting browsers such as Brave, Firefox, Tor. Use the browser in "incognito mode" when possible. Use Panopticlick, Privacy Badger or other browser tools	Don't do this. Minimize cookie usage.	S.1108 - Algorithmic Accountability Act of 2019, S. 4400National Biometric Information Privacy Act of 2020
	SURV.12	Failure to obtain consent when performing Face Recognition.	"Specifically, the panel concluded that the development of a face template using facial-recognition technology without consent (as alleged in this case) invades an individual's private affairs and concrete interests." ([84], 2019)	"In 2010, Facebook launched a feature called Tag Suggestions. If Tag Suggestions is enabled, Facebook may use facial-recognition technology to analyze whether the user's Facebook friends are in photos uploaded by that user. When a photo is uploaded, the technology scans the photo and detects whether it contains images of faces. If so, the technology extracts the various geometric data points that make a face unique, such as the distance between the eyes,nose, and ears, to create a face signature or map. The technology then compares the face signature to faces in Facebook's database of user face templates (i.e., face signatures that have already been matched to the user's profiles).2Ifthere is a match between the face signature and the face template, Facebook may suggest tagging the person in the photo." ([84], 2019)	https://cdn.ca9.uscourts.gov/datastore/opinions/2019/08/08/18-15982.pdf ([84], 2019)	No use of facial recognition without individual's consent. No use of real-time facial recognition in public setting.		S.1108 - Algorithmic Accountability Act of 2019, H.R.4978 - Online Privacy Act of 2019, S. 3861 Exposure Notification Privacy Act , S. 847 Commercial Facial Recognition Privacy Act , S. 4400National Biometric Information Privacy Act of 2020
Transparency & Communication [TRCO]	TRCO.1	Unreadable Terms of Service	People don't read Terms of Service or after trying to read them, people don't know what they mean and what they're agreeing to. Click-through consent doesn't meet the legally required condition of "knowledge" or real understanding of the Me2B deal taking place.	Terms of Service are (1) too long, (2) too complicated, (3) too filled with legal and technical jargon. 91% of people polled don't read TOS. ([47], 2017) Namedrop study participants agreed to terms giving up their unborn children, and share all data with NASA and their employers.([48], 2016)	https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 ([47], 2017) https://arstechnica.com/tech-policy/2016/07/nobody-reads-tos-agreements-even-ones-that-demand-first-born-as-payment/ ([48], 2016)	Use TOS analytical tools such as: TOSDR browser extension (https://tosdr.org/#); or https://pribot.org/polisis TOSDR browser extension (https://tosdr.org/#); or https://pribot.org/polisis	Vastly simplify Terms of Service such that a typical 13 year old [or minimum age of your service] can understand.	H.R.4978 - Online Privacy Act of 2019, H.R. 6677Application Privacy, Protection and Security (APPS) Act of 2020 , H.R. 6677Application Privacy, Protection and Security (APPS) Act of 202
	TRCO.2	Incomprehendible or difficult to find Privacy Policy. Sometimes deliberately opaque language designed to hamper real understanding	People don't have the time or capability to read lengthy, complicated, jargon-filled Privacy Policies. Click-through consent doesn't meet the legally required condition of "knowledge" or real understanding of the Me2B deal taking place.	from linked article: "...for Facebook to work as intended, it needs this sort of vague license." ([49], 2017)	https://www.howtogeek.com/304037/does-facebook-own-my-photos/ ([49], 2017) https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/ ([50], 2012)	Use TOS analytical tools such as: TOSDR browser extension (https://tosdr.org/#); or https://pribot.org/polisis TOSDR browser extension (https://tosdr.org/#); or https://pribot.org/polisis	Vastly simplify Privacy Policy such that a typical 13 year old [or minimum age of your service] can understand.	H.R.4978 - Online Privacy Act of 2019 , H.R. 5703Kids PRIVCY Act, H.R. 6677Application Privacy, Protection and Security (APPS) Act of 2020, H.R. 2013Information Transparency and Personal Data Control Act
	TRCO.3	Technology is naturally obscure to non-technical people, and suppliers don't try to breach this chasm. [Sometimes deliberate obfuscation.]	Left to "trust" the service/product vendor...	Facebook - Cambridge Analytica scandal.	https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal ([51])	Use TOS analytical tools such as: TOSDR browser extension (https://tosdr.org/#); or https://pribot.org/polisis TOSDR browser extension (https://tosdr.org/#); or https://pribot.org/polisis	Vastly simplify Privacy Policy and TOS such that a typical 13 year old [or minimum age of your service] can understand. Support the ability for people to proffer their own Deal Terms.	H.R.4978 - Online Privacy Act of 2019
Design [DSGN]	DSGN.1	Dark Patterns: ""a user interface that has been carefully crafted to trick users into doing things, such as buying insurance with their purchase or signing up for recurring bills." ([Wikipedia)	Dark patterns are deliberate manipulation through the user interface design. Suggests that you are making a decision which is not best judgement. Actively encourages self-doubt of choice..	Dialogue box choices phrased in the following manner; "Would you like information on insuring your family." O - Yes Please! I care about my family! O - No. I don't care about my family.	https://www.darkpatterns.org/types-of-dark-pattern ([52]) https://en.m.wikipedia.org/wiki/Dark_pattern ([53]) https://webtransparency.cs.princeton.edu/dark-patterns/ ([54])	Educate yourself and be mindful of when user interfaces include emotional language.	Employ a Usability Ethicist.	S. 1084 DETOUR Act
	DSGN.2	Designing in addictive characteristics.	People (especially addictive personalities) are manipulated into spending more time on digital services. Children are also particularly susceptible to these practices [Zuboff book]. "tech designers pull from a deep bag of tricks to trigger dopamine and manipulate our brains in order to maximize the time we spend on our devices." [kessler page]	Notifications when people click on "Like" buttons. Streak feature in Snapchat. Play Next mode which continues past user choice into endless playing of content without user involvement beyond first choice.	Facebook has hired design experts out of the online gambling industry to create a UI that is more addictive. https://www.vice.com/en_nz/article/vv5jkb/the-secret-ways-social-media-is-built-for-addiction ([55], 2017) https://chriskresser.com/how-a-technology-addiction-can-hurt-your-health/ ([56], 2018)	Use apps and timers to limit technology usage. In particular, put clear technology usage boundaries in place for children.	Employ a Usability Ethicist. Navigate the drive for technology usage and adoption carefully.	H.R. 5703Kids PRIVCY Act *, H.R. 5573PROTECT Kids Act , S. 1558Artificial Intelligence Initiative Act , S. 2314 Social Media Addiction Reduction Technology (SMART) Act.
	DSGN.3	Age related responsibilities: age verification,	Physical / real world connected devices and systems can cause physical harm or fatality in general. This is additionally exacerbated by inexperience and imprudence of underage users. Self serve vehicles like scooters do not generally have sufficient assurances to validate user age. This places children at risk of nefarious elements and content like porn and aggressive online behavior from adults as well as being open to cyber-stalking. [57]	1. Lime Scooter has no method to assure user is the 18+ registered user. Social apps like Instagram and Tik Tok that target younger users allow users under 13 to register for an account (they are not supposed to but no actual verification is done so users can just lie).	https://www.vox.com/2018/8/27/17676670/electric-scooter-rental-bird-lime-skip-spin-cities ([57], 2018) https://gizmodo.com/facebook-reportedly-flags-hundreds-of-thousands-of-kids-1838914363 ([58], 2019)	This may need a parent or guardian to oversee account creation - not easy to control without input from vendors to manage this	Use age verification when creating age specific accounts associated with a device.	H.R. 5703Kids PRIVCY Act , H.R. 5573PROTECT Kids Act, S. 783 Clean Slate for Kids Online Act of 2019 , The Age Discrimination Act
	DSGN.4	Not taking into account specific demographic needs around data collection, data sharing, data aggregation.	Children and other vulnerable users may need to have more focused design requirements especially around data collection, privacy policies, etc.	Some technologies, like Amazon Echo create "Kids editions" have had serious design flaws that made the user vulnerable to identity theft/cyber stalking. These should have extra care in how data is processed and handled. If a 'kids edition' of any technology is created it should be done so with extra precautions, delegate account access, etc.	Facebook Messenger chat groups - see: https://www.theverge.com/2019/7/22/20706250/facebook-messenger-kids-bug-chat-app-unauthorized-adults ([59], 2019)	Chose products that are COPPA/GDPR compliant (not always obvious) wrt age or avoid kids versions of adult products	Better design taking into account vulnerable users	H.R.4978 - Online Privacy Act of 2019, H.R. 5703Kids PRIVCY Act , S.2355 - End Racial and Religious Profiling Act of 2019
	DSGN.5	Female electronic assistants (Siri, Alexa, Cortana, etc.) propagate gender stereotypes. " - Reflecting, reinforcing and spreading gender bias - Tolerance of sexual harassment and verbal abuse - Blurring the lines between machine and human voices - The face and voice of servility and dumb mistakes" ([63], 2019)	Reinforces the stereotype that females are docile, servile. ""What emerges is an illusion that Siri – an unfeeling, unknowing, and non-human string of computer code – is a heterosexual female, tolerant and occasionally inviting of male sexual advances and even harassment," the researchers wrote. "It projects a digitally encrypted 'boys will be boys' attitude."" ([62], 2019)	Not offering voice options and/or defaulting to a gender.	https://www.pcmag.com/commentary/358057/the-real-reason-voice-assistants-are-female-and-why-it-matt ([60], 2018) https://www.wsj.com/articles/alexa-siri-cortana-the-problem-with-all-female-digital-assistants-1487709068 ([61], 2017) https://afrotech.com/united-nations-study-reveals-the-problem-with-female-voice-assistants ([62], 2019) https://unesdoc.unesco.org/ark:/48223/pf0000367416.page=1 ([63], 2019)	Select preferred gender (and accent) of Assistant in Assistant voice settings		S. 1558 Artificial Intelligence Initiative Act*

PRACTICE	ID	DESCRIPTION OF DIGITAL HARM	IMPLICATIONS FOR YOU	EXAMPLES OF UNDESIRED BEHAVIOR	CORROBORATING REFERENCES	WHAT YOU CAN DO TODAY	ME2B ALLIANCE RECOMMENDATION FOR VENDORS	LEGISLATION / BILLS
Manipulation [MNIP]	MNIP.1	Creating a social gravity by pulling users toward what is suggested or stated as "Trending" by tilting results.	Redirects people to inflated social attention spaces. By foisting importance on a social topics, "tilting" results looks to elevate those topics to artificial levels of cultural concern or urgency.	Facebook Tilting trending results in social networking platforms.	https://gizmodo.com/former-facebook-workers-we-routinely-suppressed-conser-1775461006 ([7], 2016) https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-trending-feature-shuts-down-algorithm-mark-zuckerberg-social-media-a8380681.html ([64], 2018)	Stay aware that trending may not always reflect organic results. It has not been uncommon to find human bias introduced in attempts to sway public opinion.		H.R. 5573PROTECT Kids Act *
	MNIP.2	Forcing everyone down a digital route for services	Digital identity services often forget those who do not have mobile devices or who are older or disabled and have issues with certain technologies such as ID verification processes	This is applicable to some government services that are forcing eGov route. Also commercial services that do not take wide demographic needs into account and force online only verification (crypto-platforms are guilty of this, but may have specific demography get-out for that). As online banking is pushed, closing ATMs and banks is forcing people into digital only use models.	Mobile only solutions for ID - omnichannel for ID should be accommodated for certain cross-society services such as government, banking, insurance, and similar	Not a lot the consumer can do if the vendor decides to opt for digital only user journeys	Open up your customer base by ensuring that users have choices in: the way they verify their ID, authentication credentials, with quasi-digital/offline options as needed	S. 3456 Consumer Data Privacy and Security Act , H.R. 5573PROTECT Kids Act
	MNIP.3	Humans over-anthropomorphize robots, and over-endow with human attributes such as intelligence.	Robotic companions for both children and elderly are unduly influential in unexpected and potentially harmful ways. In general, the immediate harm is that children are learning to communicate in rude ways, that bleed over into human interpersonal communication. Children learn that "please" and "thank you" aren't required when interacting with voice assistants. Due to anthropomorphization combined with voice assistants' tolerance for rudeness, children/people learn that it's okay to be rude.	"In a blog post last year, a California venture capitalist wrote that his 4-year-old daughter thought Alexa was the best speller in the house. "But I fear it's also turning our daughter into a raging a------," Hunter Walk wrote. "Because Alexa tolerates poor manners." ([67, 2019)	https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3759&context=mlr ([65], 2017) https://www.ncbi.nlm.nih.gov/pubmed/22369338 ([66], 2012) https://www.wsj.com/articles/how-google-interferes-with-its-search-algorithms-and-changes-your-results-11573823753 ([67], 2019)	Provide parental oversight to children using robots.		H.R. 5703Kids PRIVCY Act*, H.R. 5573PROTECT Kids Act
	MNIP.4	Using facial recognition to detect emotion(s) for manipulating the individual.	You may be being manipulated in ways that are not in your best interest. Moreover, using any method to detect emotion is prone to error. [2nd link in this row's references]	Employers can track employee mood.	https://nordicapis.com/20-emotion-recognition-apis-that-will-leave-you-impressed-and-concerned/ ([68], 2019) https://theoutline.com/post/8118/junk-emotion-recognition-technology?zd=1&zi=g5wgks36 ([69], 2019)	Be aware that personalized products and services are constantly creating a model of you (a "Digital Twin"), which may or may not be accurate. If there's an ability to disable personalization, you may want to do so. Turn off webcam and use a lens cover.	Recognize that emotion recognition isn't 100% accurate. Mandatory: technology must forget what they see, right after the job is done, and not use the data gathered for any purpose other than diagnostics or performance improvement. Allow users to have a "basic" non-personalized option.	S.1108 - Algorithmic Accountability Act of 2019*
	MNIP.5	Deliberate emotional manipulation.	Loss of autonomy and agency. Victim of manipulation.	Facebook's widely denigrated "experiment" with emotional manipulation.	https://www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003-users-emotions-for-science/#2aa6e3fd197c ([70], 2014)	Stay aware that use of your feedback into systems, actively as in a "Like" button, or passively such as an iris reading sensor in a headset, may be used in attempts by those systems and their interests to sway, nudge or herd you at a particularly key emotional or physical moment.		S. 3411 KIDS Act,H.R.1585 - Violence Against Women Reauthorization Act of 2019,
	MNIP.6	Exposure to influential services and products marketed without reasonable and appropriate research or understanding of impact on user(s).	You may be manipulated and impacted in ways that are not in your best interest and physiologically as well as neurologically.	A. "Kids are often an afterthought when it comes to research," said Michael Robb, director of research at Common Sense Media. "The research here is still pretty underdeveloped, which is a little concerning given how much more quickly VR is being adopted into American homes. There's a call to action for researchers to help better understand what both the short- and long-term effects are going to be on children, because right now it's like a big experiment in real time where we don't really know what's going to happen."	https://www.cnet.com/news/virtual-reality-has-a-lot-of-parents-worried-about-its-long-term-effects/ ([71], 2018)	Stay aware that use of your feedback into systems, actively as in a "Like" button, or passively such as an iris reading sensor in a headset, may be used in attempts by those systems and their interests to sway, nudge or herd you at a particularly key emotional or physical moment.		H.R. 5703Kids PRIVCY Act , S. 3411 KIDS Act , Draft United States Consumer Data Privacy Act of 2019 , S. 1558Artificial Intelligence Initiative Act
AI/ Modeling / Computation [AIMC]	AIMC.1	Computation bias negatively impacts minorities.	If you are a minority, you are likely to encounter negative impacts of bias in machine learning and AI, such being turned down for credit, or higher interest rates, similar difficulties with procuring a mortgage. Worse, the increasing use of ML in the criminal justice system is reinforcing systemic incarceration of people of color.	A. "Toxic language (e.g., hate speech, abusive speech,or other offensive speech) primarily targets members of minority groups and can catalyze real-life violence towards them..." B. "Yet something odd happened when Borden and Prater were booked into jail: A computer program spat out a score predicting the likelihood of each committing a future crime. Borden — who is black — was rated a high risk. Prater — who is white — was rated a low risk."	A. https://homes.cs.washington.edu/~msap/pdfs/sap2019risk.pdf ([72], 2019) B. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing ([73], 2016) C. https://news.berkeley.edu/story_jump/mortgage-algorithms-perpetuate-racial-bias-in-lending-study-finds/ ([74], 2018) D. https://www.ruhabenjamin.com/race-after-technology ([75], 2019)	Talk to your congresspeople. Educate your friends. Get active		S.2355 - End Racial and Religious Profiling Act of 2019, S. 847 Commercial Facial Recognition Privacy Act
	AIMC.2	Facial recognition is biased.	<< re write this>>	"The Best Algorithms Struggle to Recognize Black Faces Equally." - Racism and sexism in facial recognition	https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/ ([76], 2019)	Talk to your congresspeople. Educate your friends. Get active		S.1108 - Algorithmic Accountability Act of 2019, S.2355 - End Racial and Religious Profiling Act of 2019, S. 847 Commercial Facial Recognition Privacy Act , Draft Data Accountability and Transparency Act of 2020
	AIMC.3	Automated decision-making: What used to be human decisions [supported with technology] have evolved into purely mechanical decision-making by software. Decision making is subject to totally opaque algorithms, and deny due process.	Software can't factor in all contextual nuance. Software bears the biases of the creators and the institutional biases that produced it. Often, no way to opt out of automated decision making.	"In particular, divulging sensitive information—even to a trusted entity—may have later repercussions if laws or contracts change. For instance, when a government changes policies about health insurance or immigration, then sensitive information people disclosed under older laws (e.g., preexisting medical conditions or undocumented immigration status) could prove detrimental." [from - https://www.jstor.org/stable/10.5325/jinfopoli.8.2018.0078#n0001 ([77], 2018)]	https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3759&context=mlr ([65], 2017)	Talk to your congresspeople. Educate your friends. Get active		S.1108 - Algorithmic Accountability Act of 2019, H.R. 4978 Online Privacy Act of 2019* , S. 1558Artificial Intelligence Initiative Act
	AIMC.4	Citizen Scoring / "Scored Society"	Freedom of choice and movement is stifled based on judgement by external systems feeding off data metrics. Those metrics can be biased as certain points of view are in positions of power.	China's citizen scoring based on behavior: "China has blocked millions of "discredited" travelers from buying plane or train tickets as part of the country's controversial "social credit" system aimed at improving the behavior of citizens." ([79], 2019)	https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3759&context=mlr ([65], 2017) https://cyberlaw.stanford.edu/publications/scored-society-due-process-automated-predictions ([78], 2014) https://www.theguardian.com/world/2019/mar/01/china-bans-23m-discredited-citizens-from-buying-travel-tickets-social-credit-system ([79], 2019)	Talk to your congresspeople. Educate your friends. Get active		S.1108 - Algorithmic Accountability Act of 2019, H.R. 2231Algorithmic Accountability Act , S.2355 - End Racial and Religious Profiling Act of 2019, S. 1558Artificial Intelligence Initiative Act
	AIMC.5	Automation Bias: humans tend to trust conclusions reached by computers more than conclusions reached by humans.	"Allocating roles and functions between the human and the computer is critical in defining efficient and effective system architectures, especially in the context of human supervisory control." [80] "Human errors that result from automation bias can be further decomposed into errors of commission and omission. Automation bias errors of omission occur when humans fail to notice problems because the automation does not alert them, while errors of commission occur when humans erroneously follow automated directives or recommendation. [80]	"...in a study examining commercial pilot interaction with automation in an enroute flight planning tool, pilots, when given a computer-generated plan, exhibited significant automation over-reliance causing them to accept flight plans that were significantly sub-optimal. " [80]	"Automation Bias in Intelligent Time Critical Decision Support Systems" [link: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.91.2634&rep=rep1&type=pdf] ([80], 2012)	In cases where you may have a good sense of your intention and goal, check to see if you would agree with automated suggestions rather than simply accepting it as a better than your senses or intuition.		S.1108 - Algorithmic Accountability Act of 2019, H.R. 2231Algorithmic Accountability Act , S. 3861 Exposure Notification Privacy Act, S. 2637 Mind Your Own Business Act , S. 1558Artificial Intelligence Initiative Act
	AIMC.6	"Many large organizations rely on applicant tracking systems (ATS) to help pre-filter resumes." ([81])	"The systems work by scanning resumes for contextual keywords and key phrases, mathematically scoring them for relevance, and sending only the most qualified ones through for human review." ([81])		https://www.themuse.com/advice/beat-the-robots-how-to-get-your-resume-past-the-system-into-human-hands ([81])			S.1108 - Algorithmic Accountability Act of 2019, H.R. 2231Algorithmic Accountability Act , S. 2763- Filter Bubble Transparency Act*, S. 1558Artificial Intelligence Initiative Act
	AIMC.7	Extrapolating emotion from face recognition technology can be wrong about a person's emotional state.	Services may be personalized for you using erroneous assumptions about your emotions.	As faces are very different and nuanced, a person with certain feature characteristics and/or physical habits may be misread.	https://www.scit.net/article/418591-Amazon-says-its-facial-recognition-can-now-identify-fear-along-with-other-emotions ([7], 2019) https://theoutline.com/post/8118/junk-emotion-recognition-technology?zd=1&zi=g5wgks36 ([69], 2019)			S.1108 - Algorithmic Accountability Act of 2019, H.R. 2231Algorithmic Accountability Act ,S. 847 Commercial Facial Recognition Privacy Act , Draft Data Accountability and Transparency Act of 2020
Information Fidelity [FID]	FID.1	Search Engine result filtering.	You receive filtered information based on whatever algorithms are in place by the search engine. Your version of reality and "truth" are impacted.	Any social networking platform that does not uphold organic data results and/or impart social judgement and/or values to the filtering of information	https://www.wsj.com/articles/how-google-interferes-with-its-search-algorithms-and-changes-your-results-11573823753 ([67], 2019) https://www.youtube.com/watch?v=B8ofWFx525s ([88], 2011)	Stay aware that use of your feedback into system searches will be used in attempts by those systems and their interests to sway, nudge or herd you at a particularly key moment. Look for opportunity to use search systems and/or settings that uphold organic data results and are socially agnostic.		S. 2763- Filter Bubble Transparency Act, The Foreign Intelligence Surveillance Act (FISA)
Employer Overreach [EOR]	EOR.1	Mandated sharing of DNA information with employer.	If an employer gains access to your DNA information, they could use that information to discriminate against you.	If for instance, you are genetically predisposed to Alzheimer's and are over the age of 50, the employer may reject you.	A House committee thinks your boss should be able to see your genetic information https://www.theverge.com/2017/3/20/14880400/politics-law-bioethics-genetic-privacy-discrimination-gina-workplace-wellness ([82], 2017)			S. 1842Protecting Personal Health Data Act , Genetic Information Nondiscrimination Act of 2008 (GINA) , Health Insurance Portability and Accountability Act of 1996 (HIPAA)