Paul M. Schwartz & Daniel J. Solove

Overview of Fair Information Practice Principles (FIPPs)

Contents

Chart 1: Development and Sources of FIPPs

HEW - The Code of Fair Information Pr., 1973	The Code of Fair Information Practices of the Department of Health, Education and Welfare represents the first articulation of FIPPs. http://epic.org/privacy/consumer/code_fair_info.html
OECD - Privacy Principles, 1980	As privacy law continued to evolve, the OECD, a group of 33 leading industrial countries concerned with global economics and development, proposed their influential OECD Privacy Principles. http://oecdprivacy.org/
APEC - Privacy Frame-work, 2005	APEC, an organization of 21 Pacific Rim countries, introduced FIPPs in order to enable multinational businesses to implement uniform approaches to the use of personal data. The resulting guidelines strongly reflect the OECD Privacy Principles. http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx
DHS - Fair Information Practice Princ., 2008	The Privacy Office at the Department of Homeland Security's FIPPs resemble the OECD Privacy Principles as well. http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf
White House - Consumer Privacy Bill of Rights, 2012	The Consumer Privacy Bill of Rights published by the White House aims to apply comprehensive and globally recognized FIPPs for purposes of consumer protection. https://Obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf
FTC - Privacy Framework and Impl. R., 2012	Recently, the Federal Trade Commission issued a major report about privacy, which also included FIPPs. http://ftc.gov/os/2012/03/120326privacyreport.pdf
Privacy Act, 1974	Among the early statutes that include FIPPs is the Privacy Act. It regulates the collection, use, and disclosure of personal data by federal agencies. (5 USC § 552a)
HIPAA, 1996	Pursuant to HIPAA, the Department of Health and Human Services promulgated regulations of the privacy and security of medical information. (45 CFR §§ 160, 162, 164)
Gramm–Leach–Bliley Act (GLB), 1999	The GLB Act seeks both to facilitate data sharing among financial institutions and their affiliates and to protect customer privacy. It contains FIPPs as well. (15 USC § 6801 et seq., 16 CFR §§ 313, 314)
PIPEDA (Schedule 1), 2000	PIPEDA is a Canadian privacy statute that regulates all private-sector entities that collect personal information on Canadians and personal information used in connection with any commercial activity. http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html
EU Directive - EU Data Protection Directive, 1995	The EU Data Protection Directive's goal is to facilitate the free flow of personal information within the EU by establishing an equally high privacy level in all Member States. It is not directly binding, but implemented on the national level by each country. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML
EU Regulation - EU General Data Protection Regulation, 2016	The EU General Data Protection Regulation is the proposed successor to the EU Data Protection Directive. It seeks to update privacy law within the EU with a single law that will be immediately binding on all EU member states. http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf
NAI Code of Conduct (Section II.), 2020	The Network Advertising Initiative (NAI), an industry trade group, develops self-regulatory standards for online advertising, among which are the NAI Code of Conduct. https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf
AICPA Privacy Management Framework, 2020	The American Institute of CPAs (AICPA) and the Canadian Institute of Chartered Accountants (CICA) developed a set of FIPPs to be used by companies in their self-regulation of privacy. It was revised in 2009 and renamed GAPP. In 2020 it was updated as the Privacy Management Framework. https://www.aicpa.org/interestareas/informationtechnology/privacy-management-framework.html
DAA Self-Regulatory Princ. for OBA, 2009	The Digital Advertising Alliance (DAA) is an organization that provides a self-regulatory FIPPs regime for interest-based advertising. https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/seven-principles-07-01-09.pdf
GSMA Mobile Privacy Principles, 2012	The GSMA is an association of mobile operators and related companies devoted to supporting the standardization, deployment, and promotion of the GSM mobile telephone system. It also released a self-regulatory framework containing FIPPs. https://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf

Chart 2a: FIPPs Comparison - Frameworks & Statutes

A. Data Accuracy, Completeness, Updates

HEW - The Code of Fair Information Practices (1973)	OECD - Privacy Principles (1980)	APEC - Privacy Framework (2005)	DHS - Fair Information Practice Principles (2008)	The White House - Consumer Privacy Bill of Rights (2012)	FTC - Privacy Framework and Implementation Recommendation (2012)	
N/A	2. "Personal data should be … accurate, complete and kept up-to-date."	VI. "Personal information should be accurate, complete and kept up-to-date ...."	Data Quality and Integrity: "DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete."	5. "Companies should use reasonable measures to ensure they maintain accurate personal data."	Privacy by Design - A. Final Principle: "Companies should incorporate substantive privacy protections into their practices, such as ... data accuracy."	*continuing on next page*

	Privacy Act (5 USC § 552a) (1974)	HIPAA (45 CFR §§ 160, 162, 164) (1996)	Gramm–Leach–Bliley Act (15 USC § 6801 et seq., 16 CFR §§ 313, 314) (1999)	PIPEDA (Schedule 1) (2000)	EU Data Protection Directive (1995)	EU General Data Protection Regulation (2016)
	(c) "Each agency ... shall (1) ... keep an accurate accounting of [certain disclosures]; ... and (4) inform any person or other agency about any correction ...."	N/A	N/A	4.6 Principle 6: "Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used."	Art. 6: 1. "[P]ersonal data must be: … (d) accurate and … kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete … are erased or rectified; ...."	Art. 5: "Personal data shall be: … (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate … are erased or rectified without delay; ...."

B. Purpose, Context Limitation, Minimization

HEW - The Code of Fair Information Practices (1973)	OECD - Privacy Principles (1980)	APEC - Privacy Framework (2005)	DHS - Fair Information Practice Principles (2008)	The White House - Consumer Privacy Bill of Rights (2012)	FTC - Privacy Framework and Implementation Recommendation (2012)	
3. "There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent."	2. "Personal data should be relevant to the purposes for which they are to be used ...." 3. "[Use of personal data should be] limited to the fulfilment of those purposes [for which they were collected] or such others as are not incompatible with those purposes ...."	III. "The collection of personal information should be limited to information that is relevant to the purposes of collection ...." IV. "[Subject to consent and other exceptions p]ersonal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes ...."	Purpose Specification: "DHS should ... articulate the purpose or purposes for which the PII is intended to be used." Data Minimization: "DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) ...." Use Limitation: "DHS should use PII solely for the purpose(s) specified in the notice."	3. "Companies should limit ... use and disclosure ... to ... purposes ... consistent with ... the consumer[] [relationship] and the [disclosure] context ...." 6. "Companies should collect only as much personal data as they need to accomplish purposes specified [at 3.]."	Simplified Consumer Choice - B. Final Principle: "Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes."	*continuing on next page*

Privacy Act (5 USC § 552a) (1974)	HIPAA (45 CFR §§ 160, 162, 164) (1996)	Gramm–Leach–Bliley Act (15 USC § 6801 et seq., 16 CFR §§ 313, 314) (1999)	PIPEDA (Schedule 1) (2000)	EU Data Protection Directive (1995)	EU General Data Protection Regulation (2016)
(e) "Each agency ... shall (1) maintain ... only such information ... as is relevant and necessary ... ; (3) inform each individual ... (B) [of] the ... purpose … for which the information is intended to be used; ... [and] (11) ... publish in the Federal Register notice of any new use ...."	§ 164.502(b) "When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." (See also § 164.514(d).)	§ 6802(c) "[N]onaffiliated third part[ies receiving] ... information ... shall not ... disclose [those] to [other] nonaffiliated third part[ies]." § 6802(d) "[Subject to exceptions, a] financial institution shall not disclose ... an account number or similar [financial information] to any nonaffiliated third party for [marketing use]." (For details, see 16 CFR § 313.10 et seq.)	4.2 Principle 2: "The [collection] purposes ... shall be identified ... at or before the time [of collection]." 4.4 Principle 4: "The collection ... shall be limited to ... the purposes identified by the organization." 4.5 Principle 5: "[Subject to exceptions, p]ersonal information shall not be used or disclosed for ... other than [collection purposes] ...."	Art. 6: 1. "[P]ersonal data must be: … (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes….; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; ...."	Art. 5: "Personal data shall be: … (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; (c) adequate, relevant and limited to what is necessary in relation to the purposes ...;"

C. Notice, Choice, Consent, Control

HEW - The Code of Fair Information Practices (1973)	OECD - Privacy Principles (1980)	APEC - Privacy Framework (2005)	DHS - Fair Information Practice Principles (2008)	The White House - Consumer Privacy Bill of Rights (2012)	FTC - Privacy Framework and Implementation Recommendation (2012)	
3. "There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent."	1. "There should be limits to the collection of personal data and any such data should be obtained … with the knowledge or consent of the data subject." 4. "[Subject to consent and other exceptions, p]ersonal data should not be disclosed, made available or otherwise used for purposes other than those specified ...."	III. "[A]ny [collected personal] information should be obtained … with notice to, or consent of, the individual concerned." V. "[I]ndividuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information."	Transparency: "DHS should ... provide notice to the individual regarding its collection, use, dissemination, and maintenance of [PII]." Individual Participation: "DHS should ... to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII."	1. "Consumers have a right to exercise control over what personal data companies collect ... and how they use it.... Companies should offer consumers clear and simple choices, presented at times and in ways that enable consumers to make meaningful decisions about personal data collection, use, and disclosure."	Simplified Consumer Choice - Baseline Principle: "[S]implify consumer choice." A. Final Principle: "Companies do not need to provide choice [for practices in] context of the transaction or the company's relationship with the consumer ...." B. Final Principle: "[C]ompanies should offer the choice at a time and in a context in which the consumer is making a decision ...."	*continuing on next page*

Privacy Act (5 USC § 552a) (1974)	HIPAA (45 CFR §§ 160, 162, 164) (1996)	Gramm–Leach–Bliley Act (15 USC § 6801 et seq., 16 CFR §§ 313, 314) (1999)	PIPEDA (Schedule 1) (2000)	EU Data Protection Directive (1995)	EU General Data Protection Regulation (2016)
(b) "No agency shall disclose any record ... except ... with the prior written consent of ... the individual to whom the record pertains [or if other exceptions apply]."	§ 164.508(a)(1) "Except as otherwise permitted or required ..., a covered entity may not use or disclose protected health information without an authorization [by the treated individual]."	§ 6802(a) "[Subject to exceptions], a financial institution may not ... disclose [customer] information, unless [it notifies the customer]." (See § 6803.) § 6802(b) "A financial institution may not disclose ... [consumer] information ... unless [it] discloses to the consumer [the opt out possibility and gives notice]." (See § 6804.) (For details, see 16 CFR § 313.4 et seq.)	4.3 Principle 3: "The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate." 4.3.2 "To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand ...."	Art. 7: "[P]ersonal data may be processed only if: (a) the data subject has unambiguously given his consent; or [(b)-(f) it is necessary in certain enumerated situations]." (See Art. 8 for consenting to the processing of sensitive personal data.)	Art. 6: 1. "Processing [of personal data] shall be lawful only if ... : (a) the data subject has given consent ... for ... specific purposes; [or processing is necessary in certain enumerated situations]." (See also Art. 7 for conditions for consent, Art. 8 for processing personal information of a child, Art. 9 for processing of special categories of personal data, and Art. 21 for the right to object.)

D. Data Security, Integrity, Retention

HEW - The Code of Fair Information Practices (1973)	OECD - Privacy Principles (1980)	APEC - Privacy Framework (2005)	DHS - Fair Information Practice Principles (2008)	The White House - Consumer Privacy Bill of Rights (2012)	FTC - Privacy Framework and Implementation Recommendation (2012)	
5. "Any organization ... must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data."	5. "Personal data should be protected by reasonable security safeguards ...."	I. "[I]nformation protection should ... prevent the misuse of [personal] information.... [It] should take account of [the] risk [of misuse] ...." VII. "[I]nformation controllers should protect personal information ... with appropriate safeguards .... Such safeguards should be proportional ...."	Data Minimization: "DHS should only ... retain PII for as long as necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules ...." Security: "DHS should protect PII ... through appropriate security safeguards against risks ...."	4. "Consumers have a right to secure and responsible handling of personal data. Companies should assess the ... risks associated with their personal data practices and maintain reasonable safeguards to control risks ...." 6. "Companies should securely dispose of or de-identify personal data once they no longer need it ...."	Privacy by Design - A. Final Principle: "Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices ...."	*continuing on next page*

	Privacy Act (5 USC § 552a) (1974)	HIPAA (45 CFR §§ 160, 162, 164) (1996)	Gramm–Leach–Bliley Act (15 USC § 6801 et seq., 16 CFR §§ 313, 314) (1999)	PIPEDA (Schedule 1) (2000)	EU Data Protection Directive (1995)	EU General Data Protection Regulation (2016)
	(c) "[Subject to exceptions, e]ach agency ... shall ... (2) retain [an] accounting [of disclosures] ...." (e) "Each agency ... shall ... (10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records ...."	§ 164.530(c)(1) "A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." (See generally § 164.302 et seq.)	16 CFR § 314.3(a) "[Financial institutions] shall develop, implement, and maintain a comprehensive information security program ...." (See all details in 16 CFR § 314)	4.7 Principle 7: "Personal information shall be protected by security safeguards appropriate to the sensitivity of the information." 4.7.3 "The methods of protection should include (a) physical ... ; (b) organizational … ; and (c) technological measures ...."	Art. 17: 1. "[T]he controller must implement appropriate technical and organizational measures to protect personal data .... [S]uch measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."	Art. 32: 1. "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk ...."

E. Transparency, Openness, Education

HEW - The Code of Fair Information Practices (1973)	OECD - Privacy Principles (1980)	APEC - Privacy Framework (2005)	DHS - Fair Information Practice Principles (2008)	The White House - Consumer Privacy Bill of Rights (2012)	FTC - Privacy Framework and Implementation Recommendation (2012)	
1. "There must be no personal data record-keeping systems whose very existence is secret."	6. "There should be a general policy of openness about developments, practices and policies with respect to personal data."	II. "Personal information controllers should provide … statements about their practices and policies … that should include: a) the fact that personal information is being collected; b) the purposes for which personal information is collected; … [and further information]."	Transparency: "DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII)."	2. "Consumers have a right to … information about privacy and security practices. … [C]ompanies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it ... [and further information]."	Transparency - Baseline Principle: "Companies should increase the transparency of their data practices." A. Final Principle: "Privacy notices should be clearer, shorter, and more standardized ...." C. Final Principle: "All stakeholders should expand their efforts to educate consumers ...."	*continuing on next page*

Privacy Act (5 USC § 552a) (1974)	HIPAA (45 CFR §§ 160, 162, 164) (1996)	Gramm–Leach–Bliley Act (15 USC § 6801 et seq., 16 CFR §§ 313, 314) (1999)	PIPEDA (Schedule 1) (2000)	EU Data Protection Directive (1995)	EU General Data Protection Regulation (2016)
(e) "Each agency that maintains a system of records shall … (4) ... publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records ...."	§ 164.520(a)(1) "[Subject to exceptions], an individual has a right to adequate notice of the uses and disclosures of protected health information ... , and of the individual's rights and the covered entity's legal duties …." (Details in § 164.520(b).) § 164.530(i)(1) "A covered entity must implement policies and procedures with respect to protected health information ...."	N/A	4.8 Principle 8: 4.8.1 "Organizations shall be open about their policies and practices with respect to the management of personal information." 4.8.2 "The information made available shall include (a) [contact details to inquire about policies and practices], (b) the means of gaining access to personal information … [and further information]."	Art. 10: "[T]he controller or his representative must provide a data subject … with at least the following information … : (a) the identity of the controller … ; (b) the purposes of the processing … ; (c) … further information …." (See Art. 11 for the case where information was not obtained from the data subject.)	Art. 12: 1. "The controller shall take appropriate measures to provide ... information [about data processing] ... in a concise, transparent and easily accessible form ...." Art. 13: 1. "[It shall] provide the data subject with the following information: (a) the identity … of the controller …; (b) the contact details of the data protection officer…; [and further information]." (See also Art. 14.)

F. Data Access, Correction, Deletion

HEW - The Code of Fair Information Practices (1973)	OECD - Privacy Principles (1980)	APEC - Privacy Framework (2005)	DHS - Fair Information Practice Principles (2008)	The White House - Consumer Privacy Bill of Rights (2012)	FTC - Privacy Framework and Implementation Recommendation (2012)	
2. "There must be a way for a person to find out what information about the person is in a record and how it is used." 4. "There must be a way for a person to correct or amend a record of identifiable information about the person."	7. "An individual should have the right: a) to obtain from a data controller … confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him … ; … d) to challenge data relating to him and … to have the data erased, rectified, completed or amended."	VIII. "Individuals should be able to: a) obtain ... confirmation of whether or not the personal information controller holds personal information about them; b) have communicated to them … personal information about them; … and, c) challenge [their] accuracy … [and] have the information rectified, completed, amended or deleted."	Individual Participation: "DHS should … provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII."	5. "Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate."	Transparency - B. Final Principle: "Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use."	*continuing on next page*

Privacy Act (5 USC § 552a) (1974)	HIPAA (45 CFR §§ 160, 162, 164) (1996)	Gramm–Leach–Bliley Act (15 USC § 6801 et seq., 16 CFR §§ 313, 314) (1999)	PIPEDA (Schedule 1) (2000)	EU Data Protection Directive (1995)	EU General Data Protection Regulation (2016)
(c) "[Subject to exceptions, e]ach agency ... shall ... (3) ... make [an accounting of disclosures] available to the individual named in the record ...; and (4) inform any person ... about any correction ...." (d) "Each agency ... shall (1) [permit an] individual ... to review the record ...; (2) permit the individual to request amendment of a record ...."	§ 164.524(a)(1) "[Subject to exceptions], an individual has a right of access to inspect and obtain a copy of protected health information ...." § 164.526(a)(1) "An individual has the right to have a covered entity amend protected health information ...."	N/A	4.9 Principle 9: "Upon request, an individual ... shall be given access to [collected] information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate."	Art. 12: "Member States shall guarantee every data subject the right to obtain from the controller: (a) … confirmation as to whether or not data relating to him are being processed and information … [as] to whom the data are disclosed, communication to him … of the data … and of any available information as to their source … (b) as appropriate the rectification, erasure or blocking of data ...."	Art. 15: 1. "The data subject shall have the right to obtain ... confirmation as to whether ... her [data] are being processed.... 3. The controller shall provide ... [the] data ...." Art. 16: "The data subject shall have the right to obtain ... rectification ... [and completion of] personal data...." Art. 17: 1. "The data subject shall have the right to ... erasure of [her] data ..." Art. 18: "The data subject shall have the right to ... restriction of processing [when certain re-

						quirements are met] ....”

G. Accountability, Liability, Remedies, Auditing

HEW - The Code of Fair Information Practices (1973)	OECD - Privacy Principles (1980)	APEC - Privacy Framework (2005)	DHS - Fair Information Practice Principles (2008)	The White House - Consumer Privacy Bill of Rights (2012)	FTC - Privacy Framework and Implementation Recommendation (2012)	
N/A	8. "A data controller should be accountable for complying with measures which give effect to the [Privacy] principles ...."	IX. "A personal information controller should be accountable for complying with measures that give effect to the [APEC Fair Information] Principles ...."	Accountability and Auditing: "DHS should be accountable for complying with these principles … and auditing the … use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements."	7. "Companies should be accountable to enforcement authorities and consumers for adhering to [the Consumer Privacy Bill of Rights]."	Privacy by Design - B. Final Principle: "Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services."	*continuing on next page*

Privacy Act (5 USC § 552a) (1974)	HIPAA (45 CFR §§ 160, 162, 164) (1996)	Gramm–Leach–Bliley Act (15 USC § 6801 et seq., 16 CFR §§ 313, 314) (1999)	PIPEDA (Schedule 1) (2000)	EU Data Protection Directive (1995)	EU General Data Protection Regulation (2016)
(g)(1) "Whenever any agency ... (C) fails to maintain any record concerning any individual with ... accuracy, ... the individual may bring a civil action against the agency ...." (i)(1) "Any officer or employee of an agency, who ... willfully discloses ... material in any manner to any[one] not entitled to receive it, shall be guilty of a misdemeanor ...."	§ 160.310(a) "A covered entity must keep ... records and submit … compliance reports ...." § 164.528(a)(1) "An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity ...." (42 USC § 1320d-5 and 42 USC § 1320d-6 contain civil and criminal penalties.) (See also § 160.400 et seq.)	§ 6823(a) "Whoever knowingly and intentionally violates, or … attempts to violate, section 6821 of this title [on obtaining customer information by false pretenses] shall be fined … or imprisoned for not more than 5 years, or both."	4.1. Principle 1: 4.1.3 "An organization is responsible for personal information in its possession … including information ... transferred to a third party ...." 4.1.4 "Organizations shall implement policies and practices to give effect to the principles ...." 4.10 Principle 10: "An individual shall be able to address a challenge concerning compliance with the ... principles ...."	Art. 23: 1. "Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered." (For more, see Arts. 22, 24.)	Art. 5: 2. "The controller shall be responsible for, and be able to demonstrate compliance with [this Regulation] ...." Art. 82: 1. "Any person who has suffered ... damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or the processor ...." (For more, see Arts. 77–84.)

H. Matching, Profiling

HEW - The Code of Fair Information Practices (1973)	OECD - Privacy Principles (1980)	APEC - Privacy Framework (2005)	DHS - Fair Information Practice Principles (2008)	The White House - Consumer Privacy Bill of Rights (2012)	FTC - Privacy Framework and Implementation Recommendation (2012)	
N/A	N/A	N/A	N/A	N/A	N/A	*continuing on next page*

	Privacy Act (5 USC § 552a) (1974)	HIPAA (45 CFR §§ 160, 162, 164) (1996)	Gramm–Leach–Bliley Act (15 USC § 6801 et seq., 16 CFR §§ 313, 314) (1999)	PIPEDA (Schedule 1) (2000)	EU Data Protection Directive (1995)	EU General Data Protection Regulation (2016)
	(o)(1) "No record ... may be disclosed to a recipient agency or non-Federal agency for use in a computer matching program except pursuant to a written agreement ... specifying [the purpose and other restrictions]."	N/A	N/A	N/A	Art. 15: 1. "Member States shall grant the right to every person not to be subject to a decision which produces legal effects ... and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."	Art. 22: 1. "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects ... or similarly significantly affects [her]."

I. Data Breach Notification

HEW - The Code of Fair Information Practices (1973)	OECD - Privacy Principles (1980)	APEC - Privacy Framework (2005)	DHS - Fair Information Practice Principles (2008)	The White House - Consumer Privacy Bill of Rights (2012)	FTC - Privacy Framework and Implementation Recommendation (2012)	
N/A	N/A	N/A	N/A	N/A	N/A	*continuing on next page*

Privacy Act (5 USC § 552a) (1974)	HIPAA (45 CFR §§ 160, 162, 164) (1996)	Gramm–Leach–Bliley Act (15 USC § 6801 et seq., 16 CFR §§ 313, 314) (1999)	PIPEDA (Schedule 1) (2000)	EU Data Protection Directive (1995)	EU General Data Protection Regulation (2016)
N/A	§ 164.404(a)(1) "A covered entity shall ... notify each individual whose unsecured protected health information has been, or is reasonably believed ... to have been, accessed, acquired, used, or disclosed as a result of [a data] breach." (See generally § 164.400 et seq. for further breach requirements.)	N/A	N/A	N/A	Art. 34: 1. "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."

J. Data Portability

HEW - The Code of Fair Information Practices (1973)	OECD - Privacy Principles (1980)	APEC - Privacy Framework (2005)	DHS - Fair Information Practice Principles (2008)	The White House - Consumer Privacy Bill of Rights (2012)	FTC - Privacy Framework and Implementation Recommendation (2012)	
N/A	N/A	N/A	N/A	N/A	N/A	*continuing on next page*

Privacy Act (5 USC § 552a) (1974)	HIPAA (45 CFR §§ 160, 162, 164) (1996)	Gramm–Leach–Bliley Act (15 USC § 6801 et seq., 16 CFR §§ 313, 314) (1999)	PIPEDA (Schedule 1) (2000)	EU Data Protection Directive (1995)	EU General Data Protection Regulation (2016)
N/A	N/A	N/A	N/A	N/A	Art. 20: 2. "The data subject shall have the right to receive the personal data concerning ... [her and] to transmit those data to another controller without hindrance ...."

K. Privacy by Design

HEW - The Code of Fair Information Practices (1973)	OECD - Privacy Principles (1980)	APEC - Privacy Framework (2005)	DHS - Fair Information Practice Principles (2008)	The White House - Consumer Privacy Bill of Rights (2012)	FTC - Privacy Framework and Implementation Recommendation (2012)	
N/A	N/A	N/A	N/A	N/A	Privacy by Design - Baseline Principle: "Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services."	*continuing on next page*

Privacy Act (5 USC § 552a) (1974)	HIPAA (45 CFR §§ 160, 162, 164) (1996)	Gramm–Leach–Bliley Act (15 USC § 6801 et seq., 16 CFR §§ 313, 314) (1999)	PIPEDA (Schedule 1) (2000)	EU Data Protection Directive (1995)	EU General Data Protection Regulation (2016)
N/A	N/A	N/A	N/A	N/A	Art. 25: 1. "The controller shall ... implement appropriate technical and organizational measures ... which are designed to implement data-protection principles ... [to] protect the rights of data subjects."

Chart 2b: FIPPs Comparison - Self Regulation

A. Data Accuracy, Completeness, Updates

NAI Code of Conduct (Section II.) (2020)	AICPA Privacy Management Framework (2020)	DAA Self-Regulatory Principles for Online Behavioral Advertising (2009)	GSMA Mobile Privacy Principles (2012)
II.F.2. "Members shall conduct appropriate due diligence to help ensure that they obtain data ... from responsible sources that provide users with appropriate levels of notice and choice."	8. "The entity maintains accurate, complete and relevant PI for the purposes identified in the notice and protects the representational integrity of the PI in its ongoing interactions with data subjects."	N/A	N/A

B. Purpose, Context Limitation, Minimization

NAI Code of Conduct (Section II.) (2020)	AICPA Privacy Management Framework (2020)	DAA Self-Regulatory Principles for Online Behavioral Advertising (2009)	GSMA Mobile Privacy Principles (2012)
II.D. [Contains various use limitations for advertisement.] II.E. [Contains various transfer and service restrictions.] II.F.4. "Members shall retain DII and PII collected for use in [certain advertising practices] only as long as necessary for the purpose for which the data was collected, to fulfill another legitimate business need, or as required by law."	2. "The entity ... offers choices ..., including ... purposes for which the entity seeks to obtain and use a data subject's PI." 3. The entity collects and creates PI only for ... purposes ... in its agreements ... and ... communications with and notices provided to data subjects." 4. "The entity limits the use of PI to the purposes ... in the formal agreements/notices, and for which [there is] consent." 6. "The entity discloses PI to third parties only for the purposes ... in ... agreements and [the] notice and with ... consent."	IV.B. "Entities should retain data that is collected and used ... only as long as necessary to fulfill a legitimate business need, or as required by law."	Purpose and Use: "The access, collection, sharing, disclosure and further use of users' personal information shall be limited to meeting legitimate business purposes ...."

C. Notice, Choice, Consent, Control

NAI Code of Conduct (Section II.) (2020)	AICPA Privacy Management Framework (2020)	DAA Self-Regulatory Principles for Online Behavioral Advertising (2009)	GSMA Mobile Privacy Principles (2012)
II.B.1. "Each member company [engaged in certain advertising practices] shall provide clear, meaningful, and prominent notice on its website that describes its data collection, transfer, and use practices." (II.B.4. contains a notice requirement for cooperating websites.) II.C.1. "The level of choice that members must provide is commensurate with the sensitivity and intended use of the data."	2. "The entity ... notifies ... and offers choices when seeking ... consents, including reasons why and purposes for which the entity seeks to obtain and use ... PI." 4. "The entity limits the use of PI to the purposes ... in the formal agreements/notices, and for which a data subject has provided ... consent." 6. "The entity discloses PI to third parties only for the purposes identified in ... privacy agreements and ... notice and with the ... consent of the data subject."	II.A.1. "Third Parties and Service Providers should give ... notice ... that describes their ... data collection and use practices." (See also II.A.2. and II.B.) III.A. "A Third Party should provide consumers with the ability to exercise choice with respect to the collection and use [or transfer] of data ...." III.B.1. "Service Providers should not collect and use data ... without Consent." V. "Entities should obtain Consent before applying any material change to their ... data collection ...."	User Choice and Control: "Users shall be given opportunities to exercise meaningful choice, and control over their personal information." Respect User Rights: "Users should be provided with information about, and an easy means to exercise, their rights over the use of their personal information."

D. Data Security, Integrity, Retention

NAI Code of Conduct (Section II.) (2020)	AICPA Privacy Management Framework (2020)	DAA Self-Regulatory Principles for Online Behavioral Advertising (2009)	GSMA Mobile Privacy Principles (2012)
II.F.3. "Members that collect, transfer, or store data [for certain advertising purposes] shall provide reasonable security measures to protect that data." II.F.4. "Members [engaged in certain types of advertising] shall retain DII and PII collected for [these activities] only as long as necessary for the purpose for which the data was collected, to fulfill another legitimate business need, or as required by law."	4. "The entity retains PI for the time necessary to fulfill the stated purposes identified in the formal agreements/notices or as required by laws or regulations...." 7. "The entity protects PI against unauthorized access, removal, alteration, destruction and disclosure (both physical and logical)."	IV.A. "Entities should maintain appropriate physical, electronic, and administrative safeguards to protect the data collected and used for Online Behavioral Advertising purposes."	Security: "Personal information must be protected, using reasonable safeguards appropriate to the sensitivity of the information." Data Minimisation and Retention: "Only the minimum personal information necessary to meet legitimate business purposes ... should be collected .... Personal information must not be kept for longer than is necessary for those legitimate business purposes or to meet legal obligations and should subsequently be deleted or rendered anonymous."

E. Transparency, Openness, Education

NAI Code of Conduct (Section II.) (2020)	AICPA Privacy Management Framework (2020)	DAA Self-Regulatory Principles for Online Behavioral Advertising (2009)	GSMA Mobile Privacy Principles (2012)
II.A.2. "Members shall use reasonable efforts to educate users about Tailored Advertising and the choices available ... with respect to Tailored Advertising."	N/A	I. "Entities should participate in efforts to educate ... about Online Behavioral Advertising, including the actors in the ecosystem, how data may be collected, and how consumer choice and control may be exercised."	Openness, Transparency and Notice: "Users shall be provided with information about persons collecting personal information about them, the purposes of an application or service, and about the access, collection, sharing and further use of a users' [sic] personal information, including to whom their personal information may be disclosed ...." Education: "Users should be provided with information about privacy and security issues and ways to manage and protect their privacy."

F. Data Access, Correction, Deletion

NAI Code of Conduct (Section II.) (2020)	AICPA Privacy Management Framework (2020)	DAA Self-Regulatory Principles for Online Behavioral Advertising (2009)	GSMA Mobile Privacy Principles (2012)
II.F.1. "Members retaining PII for Tailored Advertising purposes shall provide users with ... [r]easonable access to PII, and other information that is associated with PII ...."	5. "The entity provides data subjects with access to their PI when requested or when asked to update and correct data errors or make changes."	N/A	N/A

G. Accountability, Liability, Remedies, Auditing

NAI Code of Conduct (Section II.) (2020)	AICPA Privacy Management Framework (2020)	DAA Self-Regulatory Principles for Online Behavioral Advertising (2009)	GSMA Mobile Privacy Principles (2012)
N/A	1. "The entity defines, formally documents, communicates and assigns responsibility and accountability for its PI privacy policies and procedures." 9. "The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes."	VII.A. "[E]ntities engaged in Online Behavioral Advertising are within the scope of the accountability programs."	Accountability and Enforcement: "All responsible persons are accountable for ensuring these principles are met."

H. Matching, Profiling; Data Breach Notification; Data Portability; Privacy by Design

NAI Code of Conduct (Section II.) (2020)	AICPA Privacy Management Framework (2020)	DAA Self-Regulatory Principles for Online Behavioral Advertising (2009)	GSMA Mobile Privacy Principles (2012)
N/A	N/A	N/A	N/A

Chart 3: Overview of which Framework, Law, and Self Regulation includes which FIPPs

Frameworks						Laws						Self Regulation			
HEW (1973)	**OECD (1980)**	**APEC (2005)**	**DHS (2008)**	**White House (2012)**	**FTC (2012)**	**Privacy Act (1974)**	**HIPAA (1996)**	**GLB Act (1999)**	**PIPEDA (2000)**	**EU Direct. (1995)**	**EU Regul. (2016)**	**NAI (2020)**	**AICPA (2020)**	**DAA (2009)**	**GSMA (2012)**
-	Data Accuracy	Data Accuracy	Data Accuracy	Data Accuracy	Data Accuracy	Data Accuracy	-	-	Data Accuracy	Data Accuracy	Data Accuracy	Data Accuracy	Data Accuracy	-	-
Purpose Limitation	Purpose Limitation	Purpose Limitation	Purpose Limitation	Purpose Limitation	Purpose Limitation	Purpose Limitation	Purpose Limitation	Purpose Limitation	Purpose Limitation	Purpose Limitation	Purpose Limitation	Purpose Limitation	Purpose Limitation	Purpose Limitation	Purpose Limitation
Consent	Consent	Consent	Consent	Consent	Consent	Consent	Consent	Consent	Consent	Consent	Consent	Consent	Consent	Consent	Consent
Data Security	Data Security	Data Security	Data Security	Data Security	Data Security	Data Security	Data Security	Data Security	Data Security	Data Security	Data Security	Data Security	Data Security	Data Security	Data Security
Trans-parency	Trans-parency	Trans-parency	Trans-parency	Trans-parency	Trans-parency	Trans-parency	Trans-parency	-	Trans-parency	Trans-parency	Trans-parency	Trans-parency	-	Trans-parency	Trans-parency
Data Access	Data Access	Data Access	Data Access	Data Access	Data Access	Data Access	Data Access	-	Data Access	Data Access	Data Access	Data Access	Data Access	-	-
-	Account-ability	Account-ability	Account-ability	Account-ability	Account-ability	Account-ability	Account-ability	Account-ability	Account-ability	Account-ability	Account-ability	-	Account-ability	Account-ability	Account-ability
-	-	-	-	-	-	Profiling	-	-	-	Profiling	Profiling	-	-	-	-
-	-	-	-	-	-	-	Data Breach Notific.	-	-	-	Data Breach Notific.	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	Data Portability	-	-	-	-
-	-	-	-	-	Privacy by Design	-	-	-	-	-	Privacy by Design	-	-	-	-

Chart 4: Overview of which FIPPs are included in each Framework, Law, and Self Regulation

Data Accuracy	Purpose Limitation	Consent	Data Security	Trans-parency	Data Access	Account-ability	Profiling	Data Breach Notification	Data Portability	Privacy by Design
	HEW	HEW	HEW	HEW	HEW					
OECD	OECD	OECD	OECD	OECD	OECD	OECD				
APEC	APEC	APEC	APEC	APEC	APEC	APEC				
DHS	DHS	DHS	DHS	DHS	DHS	DHS				
White House	White House	White House	White House	White House	White House	White House				
FTC	FTC	FTC	FTC	FTC	FTC	FTC				FTC
Privacy Act	Privacy Act	Privacy Act	Privacy Act	Privacy Act	Privacy Act	Privacy Act	Privacy Act			
	HIPAA	HIPAA	HIPAA	HIPAA	HIPAA	HIPAA		HIPAA		
	GLB Act	GLB Act	GLB Act			GLB Act				
PIPEDA	PIPEDA	PIPEDA	PIPEDA	PIPEDA	PIPEDA	PIPEDA				
EU Directive	EU Directive	EU Directive	EU Directive	EU Directive	EU Directive	EU Directive	EU Directive			
EU Regulation	EU Regulation	EU Regulation	EU Regulation	EU Regulation	EU Regulation	EU Regulation	EU Regulation	EU Regulation	EU Regulation	EU Regulation
NAI	NAI	NAI	NAI	NAI	NAI					
AICPA	AICPA	AICPA	AICPA		AICPA	AICPA				
	DAA	DAA	DAA	DAA		DAA				
	GSMA	GSMA	GSMA	GSMA		GSMA				