Kantara Initiative Advanced Notice and Consent Receipt Work Group

Response to the Federal Trade Commission Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security

Commercial Surveillance ANPR, R111004

Kantara Initiative Advanced Notice and Consent Work Group, 21 November 2022

Introduction, Open Standards Offering, and General Response

The Kantara Initiative is a 501 C (6) global community focused on improving the trustworthy use of identity and personal data. One major area of activity is composed of working groups that explore innovation and standardization, and develop good practice guidelines for the ethical, legal, and proportional collection, storage, and use of personal information and identity.

Kantara also runs world leading Identity Assurance Programs, including programs to assess conformance with the National Institute of Standards & Technology (NIST) 800-63 standards for identity privacy and security.

The Kantara Initiative Advanced Notice and Consent Receipt (ANCR) Work Group (WG) is the work group that is carrying forward an effort that has taken place over the last decade to advance user-centric data governance using standardized receipts and records that have been adopted and published by the Kantara Initiative and by the International Organization for Standardization.[1] This workgroup submits this response to the Federal Trade Commission (FTC) request for public comment on its Advanced Notice of Proposed Rulemaking (ANPR) on Commercial Surveillance and Data Security and 95 questions put forward.

The purpose of these notice and consent receipts and their associated records is directly targeted at addressing the lack of meaningful, informed, and legal notice and consent and the associated permissions online. As the continuing barrage of data breaches and unethical practices remind us daily, attaining a safe, equitable, and dynamic digital data economy and digital services is not possible without resolving the misuse of consent, including mis-used to justify the collection, use, distribution, re-use, and abuse of personal information.

Today, and as noted in many ANPR questions there takes place an active abuse of the notion of consent by dark patterns to get people to agree to terms and conditions through pop-ups, with resulting user experiences tilted toward less control, less transparency, less responsibility, and more surveillance.[2]

Our Work Group would like to contribute the Consent Receipt v1.1 specification and our latest effort in this area our Open Notice Record, Transparency Performance indicators (TPIs) and Controller Notice Credential[3]. Annexes 2 and 3 provide the ANPR references to Notice and Transparency.[4]

The Work Group created a set of open standards materials which comprise the ANCR operating framework. The materials were contributed from a location where they are freely available; and they are intended to be freely available to all, including when published by ISO.

The standard is fundamentally one of concentric human data control in which individuals have the agency to control, govern, and make secure their information throughout the lifecycle of the information. The operating framework, which can be leveraged and coordinated by regulators, ensures individuals have control over the information about themselves.

---

[1] There are two publications: The Consent Receipt Specification v1.1 which is both a Kantara specification as well as Annex B of ISO/IEC 29184 Online privacy notices and consent

[2] See Annex 1. Use of the Terms Consent in the ANPR

[3] See WG-ANCR wiki https://kantara.atlassian.net/wiki/spaces/WA/overview

[4] See Annex 2. and 3. Use of Notice and Transparency in the ANPR

The Kantara Initiative and its members are committed to building public infrastructure that supports individuals having control over information about themselves, and appreciate the value of that being achieved independent of service providers and platforms. We implore the FTC to investigate and make provisions for public infrastructure and applications that support user-centric data control through no-cost publicly accessible registries that reveal corporate transparency compliance as measured against the ANCR standard; and technical and legal requirements for browser and application functionality. We offer the ANCR standard as a way to effectively accomplish that goal since it not only addresses these critical needs, but also does so in a way that provides adequacy for cross-border data flows and governance that are critical to the competitive position of the United States in a global data economy.

The FTC can use the ANCR standard as specification for the requirements for notice, consent, and transparency information that must be provided by controllers BEFORE surveillance or data collection take place, and as a prerequisite to asking for consent, as well as prior to any processing under any justification. The associated transparency index provides consumers with an unbiased and independent measurement of data controllers' performance in information governance, privacy, and security, and the motivation for organizations to identify and improve their information management practices engendering trust and confidence of consumers, regulators, and lawmakers.

The goal of implementing the framework is to re-establish the use of meaningful notice and consent through consistent technical standards applicable in all jurisdictions, which provide interoperability of human (consumer) data rights grounded in legal requirements found across the United States in federal and state laws, and which adhere to international conventions such as the EU's General Data Protection Regulation, the Canada's Personal Information Protection and Electronic Documents Act and the requirements for notice and consent in the Council of Europe 108+ that comes into effect in 2023.

The FTC should regulate through rulemaking to establish requirements and accountability for Data Controllers or any entity that is collecting information for standardized notices and consent that facilitate personal data control, co-governance, and data security.

Notices today are not, but need to be interoperable — technically, legally, and socially — for security, privacy, and trust. To address this the FTC can and should also leverage the existing body of international interoperable privacy regulations and standards, many of which the FTC helped initiate.

The United States is not China, Russia, or North Korea where the digital world is firewalled off from consumers. Instead, here, we expect to fully engage in a global dynamic data economy.

Recommendations for Improving FTC Fair Information Practice Principle for Consumer Notice and Awareness

The first of the FTC Fair Information Practice Principles, which is globally recognized, is the need for consumer notice and awareness. The Principles need expansion, clarification, and development to identify and address the harms arising from the evolving cyber-physical world, and to ensure proper notice to consumers, and comprehensive consumer awareness about information collection, use, and handling practices.

Recommendation 1: Organizational Transparency

The currently accepted model of 'consent' approved and embraced by regulators and lawmakers permits vague language that makes it impossible for consumers to understand who is collecting their personal information, for what purposes, where in the world the date will be processed and stored, and what will ultimately happen to that data.

Consumers are relegated to consenting to the use of their information "for a variety of business purposes including" — with a list of examples, but not a definitive or limited list of purposes. Unfortunately, 'business purposes' can be construed to include all legal conduct, including activity with which the consumer has a legitimate objection, with no way to know that they are consenting to objectionable conduct and no effective recourse.

To address these harms, organizations must provide consumers with notice , stated in clear and unambiguous language, before or at the time of collecting personal information, which identifies precisely who will be collecting their information and for what specific purposes; where in the world the data will be processed and stored; with whom and what entities it will be disclosed and for what purposes; and provide a mechanism for consumers to withdraw their consent, with the organization then being responsible to return or delete the personal information from their own systems and from those of entities to which the information has been disclosed.

Consumers must be given the clear, detailed information to understand who, where, and what they are dealing with, ideally with a receipt and record created by and for the consumer:

- Without this there is no security,
- Without this there is no trust, and
- Without this there is no privacy for consumers.

This lack of security, trust, and privacy is a substantial harm, currently unavoidable to consumers, which is under the Commission's authority, and requires action.

Recommendation 2: Notice of Risk and Proof of Notice

The FTC should require 2 Factor Notice (2FN), and a requirement for measuring how performative the notice is for the consumer — the mechanics of which are both articulated in the ANCR Open Notice Record, and the Controller Notice Credential.

The 2 Factor Notice is composed of a notice of risk and a proof of notice; and both components must be offered in clear, fulsome, and unambiguous language that a consumer can understand since, without such clarity, there is no basis for individuals to grant informed consent to entities to collect, use, process or disclose personal information.

Two-factor notice drastically changes the data disclosure landscape for consumers:

- It introduces decentralized data co-governance where both consumers and regulators can enforce consumers' rights independently.
- It reduces consumer risk, increases personal data value, and the cost-effectiveness of security, privacy, and regulation.

- It benefits consumers, organizations, and the FTC with active, localized and decentralized, objective open-source intelligence, that can account for the legal/technical state of consumer surveillance and data protection.

a. *What Are the Mechanisms for Opacity*?

- Question 86. The Commission invites comment on the nature of the opacity of different forms of commercial surveillance practices. On which technological or legal mechanisms do companies rely to shield their commercial surveillance practices from public scrutiny? Intellectual property protections, including trade secrets, for example, limit the involuntary public disclosure of the assets on which companies rely to deliver products, services, content, or advertisements. How should the Commission address, if at all, these potential limitations?

The ANCR specification and protocol gives an example of the mechanisms of Opacity that is raised in ANPR Question 86, not so much in the technical or legal methods to shield scrutiny, but rather to look at specifying the requirements for transparency to obviate a need to address ways to diminish harmful opacity.

The FTC recognizes the importance of notice in rulemaking (see Annex 2 for examples of its mention). Indeed, the ANPR is testimony to the FTC formally recognizing the need for notice as an initial step in any rulemaking and decision process. Implementing a robust and standardized notice and consent regime for data in the physical and the online world — such as that provided in the ANCR Framework — must be part of any action taken before any surveillance is permitted.

Standardized, usable, and meaningful consent as described in the ANCR Framework is equally important with regards to commercial surveillance and data security. Just as notice is necessary and commonplace for lawmaking it needs to be the same to mitigate against risks to consumers that arises from data collection, use and disclosure, from commercial surveillance, and from data security to minimize risk.

Given the above, is apparent that the FTC should legislate advance notice of surveillance and data security risk to individuals; to make such notice mandatory for all browsers and all applications; to recognize privacy as a fundamental right that supersedes terms and conditions; and standardize the requirements for transparency and notice as outlined in the Kantara Initiative Advanced Notice and Consent Receipt (ANCR) work group specifications and framework.

Respectfully submitted,

Kantara Advanced Notice and Consent Work Group

Sal D'Agostino, Chair

Mark Lizar, Specification Editor

Sharon Polsky MAPP, Specification Co-Editor

November 2022

Annex 1. Use of the Word Consent in the ANPR

The word 'consent' is used in the following instances in the ANPR

Pg. 4 ostensible consent

Pg. 5 footnote 17 Commissioner Slaughter, privacy consent as illusory, no choice other than to consent

Pg. 5 footnote 19 Richards and Hartzog, The Pathologies of Digital Consent, Privacy Self-Management, and the Consent Dilemma

Pg. 6 individual consent may be irrelevant

Pg. 10 providing notice and obtaining consent

Pg. 18 existing consent order, see also Footnote 99, United States v. Twitter

Pg. 21 Footnote 114 FTC Workshop Bringing Dark Patterns to Light failure to assertively reject the service or cancel the agreement as consent.

Pg. 28 Question 19 Given the lack of clarity about the workings of commercial surveillance behind the screen or display, is parental consent an efficacious way of ensuring child online privacy?

Pg. 28 Question 21 Should new rules set out clear limits on personalized advertising to children and teenagers irrespective of parental consent?

Pg. 37 d. How, if at All, Should the Commission Regulate Harmful Commercial Surveillance or Data Security Practices that Are Prevalent? vi. Consumer Consent

Pg. 37 Question 73 The Commission invites comment on the effectiveness and administrability of consumer consent to companies' commercial surveillance and data security practices. Given the reported scale, opacity, and pervasiveness of existing commercial surveillance today, to what extent is consumer consent an effective way of evaluating whether a practice is unfair or deceptive? How should the Commission evaluate its effectiveness?

Pg. 37 Question 74 In which circumstances, if any, is consumer consent likely to be effective? Which factors, if any, determine whether consumer consent is effective?

Pg. 37 Question 75 To what extent does current law prohibit commercial surveillance practices, irrespective of whether consumers consent to them?

Pg. 37 Question 76 To what extent should new trade regulation rules prohibit certain specific commercial surveillance practices, irrespective of whether consumers consent to them?

Pg. 37, 38 Question 77 To what extent should new trade regulation rules require firms to give consumers the choice of whether to be subject to commercial surveillance? To what extent should new trade regulation rules give consumers the choice of withdrawing their duly given prior consent? How demonstrable or substantial must consumer consent be if it is to remain a useful way of evaluating whether a commercial surveillance practice is unfair or deceptive? How should the Commission evaluate whether consumer consent is meaningful enough?

Pg. 38 Question 78 What would be the effects on consumers of a rule that required firms to give consumers the choice of being subject to commercial surveillance or withdrawing that consent? When or how often should any given company offer consumers the choice? And for which practices should companies provide these options, if not all?

Pg. 38 Question 79 Should the Commission require different consent standards for different consumer groups (e.g., parents of teenagers (as opposed to parents of pre-teens), elderly individuals, individuals in crisis or otherwise especially vulnerable to deception)?

Questions 19 and 21 are specific to parental consent.

Annex 2 Use of the Word Notice in the ANPR

The use of the word 'notice' in the ANPR is both interesting and double-edged, since the ANPR is itself a notice.

Pg. 1 ACTION: Advance notice

Pg. 1 SUMMARY: publishing this advance notice.

Pg. 5 Many privacy notices that acknowledge such risks are reportedly not readable to the average consumer. Footnote 22 Brooke Auxier, et al, also Solove, McDonald & Cranor, and Pollach . Many are not even privacy notices or privacy policies but terms that hope to reduce data processor and data controller liability.

Pg. 6 Lengthy privacy notices

Pg. 10 (Also see consent reference) providing notice and obtaining consent

Pg. 10 Footnote 47 advocacy groups urged the Commission to commence a rulemaking process

Pg. 20 to provide notice to consumers affected by harmful practices.

Pg. 22 Footnote 121 Commission should provide industries notices of practices that the FTC had declared unfair or deceptive

Pg. 24 Footnote 127 and notice requirements

viii. Notice, Transparency and Disclosure under d. How, if at All, Should the Commission Regulate Harmful Commercial Surveillance or Data Security Practices that Are Prevalent?

b. Who Should Administer Notice or Disclosure Requirements?

Questions 87, and 88

c. What Should Companies Provide Notice of or Disclose?

Questions 89, 90, 91, 92, 93, and 94

Annex 3. Use of the Word Transparency in the ANPR

The word ‘transparency’ is used in the ANPR:

Pg. 4 Footnote 13 FTC: Data Brokers: A Call for Transparency and Accountability

Pg. 5 Footnote 20 FTC: Data Brokers: A Call for Transparency and Accountability

Pg. 11 Footnote 51 In 2021, the European Commission also announced proposed legislation to create additional rules for artificial intelligence that would, among other things, impose particular documentation, transparency, data management, recordkeeping, security, assessment, notification, and registration requirements for certain artificial intelligence systems that pose high risks of causing consumer injury.

Pg. 20 mandating that companies improve the transparency of the data management practices. See Footnote 111 FTC Charges Twitter Press Release

Pg. 21 Footnote 113 FTC: Data Brokers: A Call for Transparency and Accountability

Pg. 21 Footnote 119 Mobile Privacy Disclosures: Building Trust Through Transparency: FTC Staff Report

Pg. 38 vii. Notice, Transparency, and Disclosure

Pg. 39 Question 84 In which contexts are transparency or disclosure requirements effective? In which contexts are they less effective?

Pg. 40 Question 91 Disclosure requirements could vary depending on the nature of the service or potential for harm. A potential new trade regulation rule could, for example, require different kinds of disclosure tools depending on the nature of the data or practices at issue (e.g., collection, retention, or transfer) or the sector (e.g., consumer credit, housing, or work). Or the agency could impose transparency measures that require in-depth accounting (e.g., impact assessments) or evaluation against externally developed standards (e.g., third-party auditing).

Pg. 44 Because disclosing sources of funding promotes transparency... in discussing the public hearings.