Federal Trade Commission
Privacy Impact Assessment

AgileLaw

Reviewed February 2022

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC or agency) enforces competition and consumer protection laws and regulations to promote competition and protect consumers. Towards that end, FTC staff investigate proposed transactions and conduct, as well as allegations of unfair or deceptive practices in violation of the FTC Act. As part of the investigation process, FTC staff issue subpoenas and civil investigative demands seeking sworn testimony from witnesses, in the form of investigational hearings or depositions. These investigational hearings and depositions must be conducted in accordance with FTC Rules of Practice and, for federal court depositions, the Federal Rules of Civil Procedure. These investigational hearings and depositions are typically conducted by FTC staff throughout the Bureau of Competition (BC) and the Bureau of Consumer Protection (BCP).

It is critical for FTC staff to be able to continue their investigative work, even if such activities must be conducted remotely or through virtual means. To accomplish the task of conducting online depositions in a safe remote environment, the FTC uses AgileLaw, an electronic exhibit management tool used to display documents to witnesses in the course of investigational hearings and virtual depositions. AgileLaw allows parties to upload documents (typically nonpublic), and remotely share and discuss such documents with a deponent. These documents can include (but are not limited to) copies of strategic plans, marketing materials, emails, and financial information. Additionally, use of AgileLaw permits attorneys and witnesses to annotate documents and mark exhibits.

The FTC has partnered with its current stenographic services vendor, For the Record, Inc. (FTR), to utilize the AgileLaw application. FTR maintains the license and contract that allows FTC's use of AgileLaw.[1]

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The FTC is permitted by law to collect these documents, typically pursuant to a subpoena or a civil investigative demand, and use such information in the course of its investigations. Depending on the matter, these laws may include the Federal Trade Commission Act, 15 U.S.C. §§ 41-58; the Sherman Act, 15 U.S.C. § 1–7; the Clayton Act, 15 U.S.C. § 12–27, 29 U.S.C. § 52–53; the Hart-Scott-Rodino Antitrust Improvements Act, 15 U.S.C. § 18a; and the Robinson-Patman Act, 15 U.S.C. § 13. These statutes not only authorize the collection of information, but also have provisions that limit the disclosure of the data.

[1] For more information about the FTC's stenographic services, refer to the StenTrack Privacy Impact Assessment, available online.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[2] may be collected or maintained in the system/project. Check all that apply.

AgileLaw contains PII relating to system users (e.g., FTC employees, opposing (outside) counsel, witnesses) and to other individuals (e.g., investigatory targets or third parties). For the Record, Inc. facilitates setting up user accounts for authorized FTC employees on the AgileLaw platform by registering users' email addresses, which serve as the users' system IDs. Users are also required to provide their full names and create unique passwords in order to access and use AgileLaw. As noted earlier, once users have access, they may upload content to the AgileLaw application, including files, attachments, and exhibits that may contain PII, for sharing with other users on the platform. Such documents can contain any and all types of PII, as noted in the chart below. Documents are organized by case file. A unique PIN/password is generated by the system for each particular case file; this PIN is made available to those authorized individuals who require access to that specific investigation or deposition.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☒ Full Name	☒ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☒ Date of Birth	☒ Audio Recordings	☒ Internet Cookie Containing PII
☒ Home Address	☒ Photographic Identifiers (e.g., image, x-ray, video)	☒ Employment Status, History, or Information
☒ Phone Number(s)	☒ Certificates (e.g., birth, death, marriage, etc.)	☒ Employee Identification Number (EIN)
☒ Place of Birth	☒ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☒ Salary
☒ Age	☒ Vehicle Identifiers (e.g., license plates)	☒ Military Status/Records/ ID Number
☒ Race/ethnicity	☒ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☒ IP/MAC Address
☒ Alias	☒ Geolocation Information	☒ Investigation Report or Database
☒ Sex	☒ Passport Number	☒ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other *(Please Specify)*: AgileLaw will also use a unique PIN/password generated for all parties to access a specific deposition/investigational hearing.
☒ Work Address		
☒ Taxpayer ID		
☒ Credit Card Number		
☒ Facsimile Number		
☒ Medical Information		
☒ Education Records		
☒ Social Security Number		
☒ Mother's Maiden Name		

[2] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Administrative data. The system collects and stores administrative data, including the names of the FTC case file , the filenames of documents, and the names, user names, and passwords for AgileLaw users (Bureau staff, Outside Counsel, Witnesses, and For the Record, Inc).

Log data. In addition, the system collects AgileLaw user login data (Bureau staff, Outside Counsel, Witnesses, and For the Record, Inc.), including IP addresses and date and time information.

Files, attachments, and exhibits uploaded onto the system may, in some cases, include PII about individuals (e.g., names, titles, addresses, personal financial data or statements, DOB, SSN, or other information about the individual whose oral testimony is being taken or about other, third-party individuals who are the subject of such testimony).

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

Files, attachments, and exhibits uploaded and shared in the system also may include non-PII, mainly business records, such as strategic plans, marketing materials, emails, and corporate financials. These documents are typically nonpublic in nature.

Counsel is able to mark-up and provide comments on the exhibits, and the system maintains the marked-up version as a separate copy from what the witness originally submitted. These comments and mark-ups do not generally include or involve any additional PII.

2.3 What is the purpose for collection of the information listed above?

The purpose of collecting (i.e., uploading) documents that may contain PII onto AgileLaw is to permit FTC attorneys to electronically view, share, and annotate documents during remote depositions and investigational hearings. The purpose for the collection of administrative data is for the administration and security of the system (e.g., password recovery) by AgileLaw. The FTC will not be managing or monitoring passwords or system security.

2.4 What are the sources of the information in the system/project? How is the information collected?

Source of Data	***Type of Data Provided & How It Is Collected***
FTC staff	FTC staff provide their PII (e.g., full name, e-mail address) to FTR to register for system access, then upload their documents (exhibits) onto AgileLaw for use during the deposition/investigational hearing. Documents are uploaded to case-specific folders. Authorized FTC staff are provided access to folders based upon case assignments. The uploaded

Source of Data	*Type of Data Provided & How It Is Collected*
	documents are obtained from the subject (target) of the investigation or third parties.
External Counsel	External counsel working with the FTC (e.g., co-counsel from a state Attorney General's office, local counsel retained under contract) is permitted to upload documents to AgileLaw during a deposition/investigational hearing. They are permitted to mark and share those documents with the deponent/witness and with FTC counsel. The uploaded documents are obtained from the subject (target) of the investigation or third parties. External counsel must also provide their PII (name and email address) to register for access to the system.
Non-FTC Users	Opposing counsel who have their own AgileLaw account and are not using it as guests have the capability to upload documents and introduce them in a specific deposition.
System-Generated Data	AgileLaw generates and maintains the log data on system usage and users automatically.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
FTC Staff	Authorized FTC staff can access documents for use in a deposition/investigational hearing specific to a case and share such documents with the witness, co-counsel, and opposing counsel. Each FTC staff person assigned to that particular case also has the ability to view any annotations (notes) that may have been added to the originally uploaded documents.
FTC External Counsel	Authorized External Counsel working with the FTC (e.g., state Attorney General co-counsel, or local counsel retained under contract) can access documents for use in a specific deposition/investigational hearing in a particular case and may share documents with the witness, co-counsel, and opposing counsel. However, external counsel is not provided access to the case-specific folders that FTC staff use. External counsel is permitted to view only those documents that (a) external counsel uploads or (b) FTC staff reveals in AgileLaw during a specific deposition/investigational hearing.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
Non-FTC Users	Non-FTC users can view only (1) the documents FTC staff reveal in AgileLaw for a specific deposition/IH; and (2) (if external or opposing counsel, with those permissions) only the documents that external or opposing counsel upload to the specific deposition/IH.

For the Record, Inc. (FTR)	FTR issues user accounts to authorized FTC users to access the AgileLaw system and provides password assistance when needed. FTR has the ability to view documents uploaded to AgileLaw during the deposition/investigational hearing. After serving as stenographer during the deposition/investigational hearing, FTR staff download any documents used during the deposition/hearing and remove them from the AgileLaw platform.
AgileLaw	Although FTC information is stored on the AgileLaw platform, AgileLaw staff does not routinely have access to the data.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

External Counsel working with the FTC (see above) have access to documents for use in a deposition/investigational hearing in a specific case; they may share documents with the witness, co-counsel, and opposing counsel. External Counsel are required to enter into nondisclosure agreements with the FTC; for federal court cases, a court-entered protective order also supplements this requirement.

For the Record, Inc. is also able to view the documents during the deposition/investigational hearing. After serving as stenographer during the deposition/investigational hearing, FTR downloads any documents/exhibits used during the session and deletes them from the AgileLaw platform. As an FTC contractor, FTR is bound by a nondisclosure agreement with the agency that requires that such information be maintained as confidential.

AgileLaw employees do not have routine access to the contents of documents that FTC staff and/or external counsel may upload to the AgileLaw platform, which are protected by a unique security key, as described in section 3.3 below.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

In the event that any FTC data is exposed or compromised, AgileLaw maintains an incident response plan that requires immediate notification to FTR. FTR, acting as the subscription holder for AgileLaw, is responsible for reporting incidents impacting FTC documents to the Contract COR. Likewise, if an FTC contractor (e.g., local counsel retained by the FTC) with access to AgileLaw experiences an incident or breach, they must notify and cooperate with the FTC under their contract and the FTC's incident response plan.

The exhibits are stored in the AgileLaw database each with their own unique encryption key. No data is accessible, even to the service provider's servers, without this key. For Deposition sessions, no one outside of the FTC, including AgileLaw's own employees, have access to uploaded content within the application. AgileLaw grants this session encryption key only during an active user session and revokes it upon logout. A separate, isolated server process—that itself has no customer data access rights—is responsible for granting access to this key at the time of user authentication. In addition, encrypted documents are stored in a separate database for each customer, adding another layer of isolation. Storing all customer data with this separation prevents malicious or inadvertent unauthorized exposure of all data.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

☒ Notice is provided via (*check all that apply*):
- ☐ Privacy Act Statement (☐ Written ☐ Oral)
- ☒ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner
- ☒ Other (*explain*): The AgileLaw website posts their detailed privacy policy. There is a requirement to check an "I Agree" box on the user agreement when each FTC user registers his/her account. That agreement includes a reference and link to the AgileLaw privacy policy.

☐ Notice is not provided (explain): _____

AgileLaw's privacy policy on its website, agilelaw.com/privacy, informs all users of the collection of PII in connection with creation of an AgileLaw account, as well as with the use of documents that are uploaded to the AgileLaw site.

For those documents that FTC uploads to the website, the FTC provides notice to individuals about its policies regarding the use and disclosure of such documents at the time information is collected pursuant to a CID or subpoena or voluntarily in lieu thereof. Notice is provided as part of the request (e.g., in a letter request, or in the document outlining the compulsory process request). This notice may include a Privacy Act Statement, when that statute applies. See section 8.3 below.

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

Unless specified otherwise, user data required to register with AgileLaw is mandatory, and failure to provide this information may make it impossible for the user to access and upload documents, and/or participate in virtual depositions/investigational hearings via AgileLaw. This includes a valid user ID (email address), full name, and unique password to create a registered account. In certain cases where the AgileLaw application specifically states that some data is not mandatory, users are not obligated to provide the data, and it does not interfere with the availability or the functioning of the service.

For files, attachments and exhibits that are uploaded into the system, individuals whose PII may be contained in such documents may have an opportunity to decline to provide information, except information that the FTC obtains by compulsory process, which is mandatory (e.g., subpoena, CID). If the individual is the submitter of a document, the individual may be entitled to notice an opportunity to object prior to disclosure (see, e.g., section 21 of the FTC Act). Once information is provided by an individual, however, use of his or her information by the FTC (e.g., uploading it to AgileLaw) is not subject to individual consent, except as provided by law (see, e.g., routine uses under the Privacy Act of 1974, where applicable).

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Users of AgileLaw do not have access to data about themselves in the AgileLaw application, except to create or change passwords associated with their registered account.

Witnesses do not have direct access to any of the information that may be contained about them within the documents that FTC staff may have uploaded to the AgileLaw platform. Each witness is provided access only to those documents that FTC staff choose to reveal to the witness during a specific deposition or investigational hearing. Following each deposition or investigational hearing, For the Record provides a copy of the transcript, as well as any documents revealed to the witness during that session, to the witness and the witness's counsel.

Any individual who is required to submit data to the FTC or to testify in a deposition or investigational hearing may request a copy of any document it submitted under FTC Rule 2.9, 16 C.F.R. § 2.9. Individuals must follow the FTC's Privacy Act rules and procedures, which are published in the Code of Federal Regulations at 16 C.F.R. § 4.13, for requests for information. Privacy Act requests must be made in writing and submitted to the FTC's Office of General Counsel. See section 8.3 below (Privacy Act).

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

As stated above, users of AgileLaw do not have access to data about themselves in the AgileLaw application, except to change or update their account passwords. In the event a user would like to correct their name within the AgileLaw application, the user may contact For the Record to correct that information.

Witnesses do not have direct access to any PII that may be contained in documents uploaded to the AgileLaw platform. To the extent that a witness views any documents, each witness producing documents to the FTC pursuant to a subpoena or CID must attest to the accuracy of the information contained within such documents, pursuant to Section 20(c) of the FTC Act. Under the Privacy Act, see section 8.3 below, individuals may generally seek access to and correction (amendment) of records maintained and retrieved by their name or other personal identifier from an agency system of records. See Commission Rule 4.13(g), 16 C.F.R. § 4.13(g). That right will not normally apply to investigatory files, attachments, or exhibits uploaded to the AgileLaw platform, since such investigatory records are generally exempted under the Act from such rights. See Commission Rule 4.13, 16 C.F.R. § 4.13(m) (list of exempt FTC Privacy Act record systems).

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

The exhibits and other documents that are collected for use in the AgileLaw system are verified to be accurate by the submitting party, which attests to their accuracy in a sworn affidavit. Information incorporated into the AgileLaw system is subject to appropriate security and chain-of-custody controls. In addition to protecting against unauthorized access, alteration, or dissemination, these controls reduce the risk of loss and assure the integrity of the evidentiary materials from the point at which they are included in the system.

Users of AgileLaw are responsible for ensuring that any PII they submit for system access (FTC Users) and for access to specific depositions/IHs (External Counsel and Non-FTC Users) is accurate. For example, if a FTC User supplies the wrong e-mail address, registration cannot be completed and access will be denied. If a FTC User enters an incorrect password to access the system, access will be denied.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

Technical safeguards are built into the AgileLaw system to protect data from unauthorized access. Only authorized FTC staff and For the Record are granted access to the system. FTC staff log in with a username and password. The AgileLaw system terminates sessions after 30 minutes of inactivity. Staff are given access to the minimal portion of the AgileLaw platform relating to staff's specific case. All exhibits are stored in the database with its own unique key. No data is accessible, even to the service provider's servers, without this key. No one outside of the FTC, including AgileLaw's own employees, has access to this nonpublic information. AgileLaw grants this key only during an active user session and revokes it upon logout. A separate, isolated server process is responsible for granting access to this key at the time of user authentication. In addition, encrypted documents are stored in a separate database for each customer, adding another layer of isolation. Storing all customer data with this separation prevents malicious or inadvertent unauthorized exposure of all data.

For depositions in federal litigations, the deponent, deponent's counsel, and FTC staff participating in the deposition are barred from unauthorized disclosure of the information pursuant to protective orders entered in those cases. For investigational hearings, FTC staff is barred from the unauthorized disclosure of this information pursuant to the FTC's Rules of Practice, *see* 16 C.F.R. § 4.10. See also 15 U.S.C. § 50.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

There is no plan to use PII in the course of system testing, training, or research.

☒ Not Applicable

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

Once a deposition/investigational hearing has concluded, For the Record deletes electronic documents that were revealed to the witness during the deposition/investigational hearing session and initiates an archive phase that preserves the exhibits and protects them from modification within the AgileLaw system. The archiving process then stores the exhibits for seven calendar days before being permanently deleted from AgileLaw systems. The final exhibits, transcript, and any recordings are preserved as a record of the deposition/investigational hearing, and the appropriate records retention schedule is applied. As an added protection, however, by FTC instruction, FTR deletes FTC documents at the 30-calendar-day mark by established and practiced standard operating procedure.

When the FTR's contract with FTC concludes, FTR will coordinate with AgileLaw to delete any remaining FTC documents and sessions associated with the FTR account.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

Yes, the AgileLaw system can be accessed through the website, www.agilelaw.com. Any use of cookies or other tracking tools by the AgileLaw website or by the owners of third-party services used by AgileLaw is in order to carry out activities that are necessary for the operation or delivery of the application. The duration of these cookies (i.e., whether they are temporary or persistent) and what information is collected, maintained or tracked may vary.[3] The FTC has no access to this cookie or other AgileLaw tracking data. These cookies or other tracking would only affect users of AgileLaw (i.e., FTC staff, external counsel, outside counsel, witnesses) and not any individuals whose PII may be contained in documents uploaded to the site.

AgileLaw does not view the actual information in the site, including passwords, security answers, case names, case information, document names, document contents, deponent names, dates, attorney notes, annotations, exhibit numbers, or other private information entered into or uploaded to the site.

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Risk	*Mitigation Strategy*
Documents inadvertently retained in the system after the conclusion of depositions/investigational hearings	Data within the AgileLaw system is encrypted and is not directly accessible to anyone other than users with authorized access. Under current processes, FTR initiates an archive phase after the deposition is concluded and documents that were revealed to a witness from AgileLaw are stamped and saved for an additional seven days. The exhibits are stamped to ensure exhibits are not added or changed after the conclusion of the deposition. After seven days, the exhibits are removed from the AgileLaw system, the document is no longer available on AgileLaw servers.
FTC staff inadvertently reveals a document to the wrong witness during a deposition/investigational	Different roles have different levels of access. FTC staff have the ability to view the document prior to revealing it in the course of the deposition/investigational hearing. In the event FTC staff accidentally reveals the wrong document, he

[33] For more information, see AgileLaw's Cookie Policy.

Risk	*Mitigation Strategy*
hearing	or she has the ability to clawback the document, so that the witness cannot view it anymore.
Witness/opposing counsel is given the PIN/access code to the wrong AgileLaw session	Upon starting an AgileLaw session, a unique PIN is assigned that is made available to the participants. Each session has a waiting room and requires the driver (either FTC or FTR staff) to affirmatively admit each person to the session. In the event the wrong person attempts to access the session, the driver can reject admittance or, if admitted, remove the person, even if they present the PIN

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

AgileLaw is designed with privacy controls such as system lockout, and the use of a PIN to enhance the protection of personal information. Only authorized FTC staff and For the Record are granted access to the system. FTC staff log in with a username and password. The AgileLaw system terminates sessions after 30 minutes of inactivity. Staff are given access to the minimal portion of the AgileLaw platform relating to staff's specific case.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

No. AgileLaw is not considered a Privacy Act records system, and therefore no SORN is needed for that platform. For files, attachments or exhibits uploaded to AgileLaw, the FTC's SORN for investigational and other nonpublic program records applies. See FTC I-1. This SORN may be viewed on the FTC's privacy policy page at www.ftc.gov.

User names, passwords, or other user registration data collected and maintained solely by AgileLaw are not subject to the Privacy Act and do not require a SORN. Although the FTC considers that information confidential and nonpublic, the FTC's SORN for Computer Systems User Identification and Access Records (FTC VII-3) applies to system user records only for systems owned or operated by the FTC or by a third party on behalf of the FTC.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

FTC users can either upload exhibits on their own or submit them to the FTC vendor, For the Record, Inc. (FTR) for uploading into AgileLaw. Non-FTC users can neither upload exhibits on their own nor submit them to FTR for uploading into AgileLaw. Unique encryption and private PINs for each specific deposition require FTC staff to admit each deposition/hearing participant. All of these measures ensure data is collected, used, stored and disseminated correctly within the AgileLaw platform