Federal Trade Commission
Privacy Impact Assessment

A

1 System Overview

1.1 Describe the project's 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. y (e)4 rfvanal aydocumtgre typicalno6 (a)4 pub (ng eado2 (y)20 (cr3 (C)-3 (onoc)4 (um)-12 ()-22 (y)20n (s)-1 (cy)20 (pi)-ul)]TJ()4 (t)b3 (ou)-1a3 (ons

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 names1 (e)4 (lar)-1 (e)maide go. , (or)-17]TJ -0.006

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?

FTC staff	

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, 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 available as follows: Exhibit 1, Exhibit 2, Exhibit 3, Exhibit 4, Exhibit 5, Exhibit 6, Exhibit 7, Exhibit 8, Exhibit 9, Exhibit 10, Exhibit 11, Exhibit 12, Exhibit 13, Exhibit 14, Exhibit 15, Exhibit 16, Exhibit 17, Exhibit 18, Exhibit 19, Exhibit 20, Exhibit 21, Exhibit 22, Exhibit 23, Exhibit 24, Exhibit 25, Exhibit 26, Exhibit 27, Exhibit 28, Exhibit 29, Exhibit 30, Exhibit 31, Exhibit 32, Exhibit 33, Exhibit 34, Exhibit 35, Exhibit 36, Exhibit 37, Exhibit 38, Exhibit 39, Exhibit 40, Exhibit 41, Exhibit 42, Exhibit 43, Exhibit 44, Exhibit 45, Exhibit 46, Exhibit 47, Exhibit 48, Exhibit 49, Exhibit 50, Exhibit 51, Exhibit 52, Exhibit 53, Exhibit 54, Exhibit 55, Exhibit 56, Exhibit 57, Exhibit 58, Exhibit 59, Exhibit 60, Exhibit 61, Exhibit 62, Exhibit 63, Exhibit 64, Exhibit 65, Exhibit 66, Exhibit 67, Exhibit 68, Exhibit 69, Exhibit 70, Exhibit 71, Exhibit 72, Exhibit 73, Exhibit 74, Exhibit 75, Exhibit 76 -1.15p-6 (o)-4 (l)-6 (o)-10 (es)-4 ( )

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

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.[33] 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?

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, FTI 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. This 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 reveal the wrong document, h

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

hearing	or she has the ability to claw back 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(cte(N)4 (N)4 o4.02fn5-1 on4(8