



**Federal Trade Commission
Privacy Impact Assessment**

**Sprout Social
December 2020
Reviewed May 2022**

SECTION 1.0 – SPECIFIC PURPOSE OF THE FTC’S USE OF SPROUT SOCIAL

1.1 – What is the specific purpose of the agency’s use of Sprout Social, and how does that use fit with the agency’s broader mission?

The Federal Trade Commission (“FTC”) uses Sprout Social, a social media content management service, to create and schedule content on the FTC’s social media accounts, to monitor activity on these accounts (e.g., messages or posts by members of the public), and to produce analytics reports for multiple networks and profiles. The social networking accounts that the FTC may manage through Sprout Social include the agency’s accounts on Twitter, YouTube, Facebook, and LinkedIn, which are all platforms the FTC uses to promote its news, information, tips, and resources for consumers and others who may not be regular visitors to FTC websites. Social media content that the FTC may manage and post through Sprout Social is generally information that already exists on FTC.gov and FTC.gov/espanol or features relevant content from the various Bureaus and Offices of the FTC. Typical FTC social media content on Sprout Social may include but is not limited to consumer and business tips and information as well as photos, news articles and short videos.

In addition, because Sprout Social allows the FTC to measure and assess activity or traffic on its social media accounts, the FTC also has access to content from users who post or otherwise engage in public discussions on any or all of the social media platforms used by the FTC: Twitter, Facebook, YouTube, and LinkedIn. The FTC may use Sprout Social to follow discussions through specific hashtags during Twitter chats, Facebook Live events, etc.

The platform fits with the agency’s broader mission to enhance informed consumer choice and public understanding of the competitive process. The platform will help to get the agency’s messaging out to the public in a more efficient manner.

1.2 – Is the agency’s use of Sprout Social consistent with all applicable laws, regulations, and polices?

The January 21, 2009 Presidential memorandum on *Transparency and Open Government* and the OMB Director’s December 8, 2009 *Open Government Directive* call on federal departments and agencies to harness new technologies to engage with the public. Using tools like Sprout Social helps the FTC to manage and archive communication with consumers on various social media platforms, which in turn helps the FTC meet the federal guidance outlined in the directive and memorandum, including the goals of transparency, participation, and collaboration.

With respect to the information that the FTC will disseminate, or in limited instances collect, through its Sprout Social account, the FTC Act authorizes the FTC to prevent unfair and deceptive acts and practices in interstate commerce and, in furtherance of this mission, to gather, compile, and make information available in the public interest. See 15 U.S.C. 45, 46(a), (f).

SECTION 2.0 – IS THERE ANY PII THAT IS LIKELY TO BECOME AVAILABLE TO THE AGENCY THROUGH THE USE OF SPROUT SOCIAL?

2.1 – What PII will be made available to tFTC?

Sprout Social is a content management platform that allows the FTC to distribute content across multiple social media sites where the FTC maintains a presence (e.g., Facebook, Twitter, LinkedIn, etc.). When registered users log in to their Sprout Social account, they must provide an email address and password to Sprout Social. (This personal user data is not available to the FTC.)

Users who connect their other social media accounts to Sprout Social can disseminate content directly to the other platforms from Sprout Social. Any publicly available information that a consumer may include in their public social media profile will be accessible to the FTC through Sprout Social. It is up to the individual to determine how much personal information they want to make publicly available; typically, however, the person's username (whether it is their actual name or an alias) is public and will be visible to the FTC. If a member of the public posts a comment or message on one of the FTC's social media accounts, the FTC may access the content of that comment or message from that social media account or through Sprout Social, including any personally identifying information that individual has made publicly available about himself/herself.

The FTC usually monitors FTC-related keywords via Sprout Social and its other social media pages to determine the type of public attention the FTC is generating online. However, the FTC does not intend to routinely use Sprout Social to solicit, collect, maintain, or disseminate PII from members of the public. The FTC may collect limited information in specific circumstances (e.g. usernames or handles) if messages or posts directed to the FTC or its employees are deemed as threatening or violent or indicates some other potential law violation. Generally, such messages or posts would be collected directly from the specific FTC social media account itself (Twitter, Facebook, LinkedIn) and/or maintained with the individual user name or handle that identifies them, rather than through Sprout Social.

Sprout Social will primarily be used to schedule the FTC's social media posts and collect general analytical reports on a regular basis including the numbers of followers, number of retweets, etc. The Sprout Social analytics tool automatically makes other information available to the FTC (as detailed below in Section 2.2.); however, the FTC does not plan to collect or track this additional information.

2.2 – What are the sources of PII?

Members of the public are the primary source of PII for social media accounts managed through Sprout Social; this includes their user name or alias and the content of their public or private messages to the FTC, comments, or other posts on the FTC's social media accounts. As noted above, the FTC has access to only the information that users have opted to make publicly available on their profile. Sprout Social also features tools that automatically compile and make other demographic information available to the FTC about users, including sex, location, interests, and other user names or handles the FTC's followers follow. However, the FTC does not plan to collect or track this additional information, and it would only be available to the FTC

in aggregate in the form of analytics data, wherein the information is not linked or linkable to a specific individual.¹

As stated above, the FTC will not have access to PII about other users of Sprout Social, other than what may be publicly accessible. As described in the FTC's PIAs for Facebook, Twitter, and LinkedIn, the FTC's collection of PII from those accounts would be limited, if any, to comments or other postings to the FTC's accounts on those sites, and/or related personally identifying information (e.g., screen name or user handle).²

2.3 – Do the FTC's activities trigger the Paperwork Reduction Act (PRA) and, if so, how will the agency comply with the statute?

Per the OMB memorandum, *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act*, the FTC's use of Sprout Social as outlined in Section 1.1 is not a web-based interactive technology that would trigger the PRA.

SECTION 3.0 THE FTC'S INTENDED OR EXPECTED USE OF PII

3.1 – Generally, how will the agency use the PII described in Section 2.0?

As mentioned above, the FTC does not intend to use Sprout Social to solicit, collect, maintain, or disseminate PII from members of the public on a routine or regular basis. As noted earlier, in specific circumstances, the FTC may collect limited information (such as usernames or social media handles) if messages or posts directed to or at the FTC or its employees are deemed as threatening or violent or indicates some other potential law violation. In these infrequent cases, this information may be shared with FTC Security and external law enforcement authorities such as the Federal Protection Service for investigation, or, where applicable, may be used for investigational purposes within the jurisdiction of the FTC (e.g., FTC Act). Sprout Social is primarily used by the FTC to monitor the FTC's social media campaigns, publicly answer questions that consumers may send through social media, capture trends in FTC content posted on social media platforms, and collect general analytic reports such as the number of likes, retweets, shares, etc., which would not ordinarily involve any use or dissemination of PII.

3.2 – Provide specific examples of the types of uses to which the PII may be subject.

The FTC does not intend to use PII made available to it through Sprout Social, except in the limited circumstances described above. As for non-PII, in accordance with OMB memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, the FTC uses some analytical data from Sprout Social to measure the overall number of followers, number of retweets, and similar statistical information to evaluate the effectiveness of the FTC's social networking Web sites.

¹ For a list of what type of information may be provided in the analytics data, refer to the [Sprout Social website](#).

² All FTC Privacy Impact Assessments are available online at <https://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments>.

If a public figure, political figure, or influencer publicly posts about the FTC and it drives notable web traffic to the FTC's social media accounts/profiles, the post may be highlighted for reference. Also, the FTC may capture, use and store PII if there is a direct threat to an FTC employee; in such cases, the information is shared with the Federal Protection Service for law enforcement purposes.

Although the Sprout Social analytics tool automatically makes other information available to the FTC (e.g., sex, location, interests, other handles or pages followed or liked by the FTC's followers), the FTC does not plan to collect or track this additional information, which is normally in aggregated, non-identifiable form, as noted earlier, and thus does not constitute PII.

SECTION 4.0 SHARING OR DISCLOSING OF PII

4.1 – With what entities or persons inside or outside the agency will the PII be shared, and for what purposes will the PII be disclosed?

As noted above, in those limited instances where the FTC may collect PII (e.g., user name or handle of a member of the public) from a social media account managed through Sprout Social, that information may be shared with FTC security or other law enforcement agencies, including the Federal Protective Service, or used internally for law enforcement investigatory purposes, if appropriate. Otherwise, PII will not be routinely collected or shared via Sprout Social.

4.2 – What safeguards are in place to prevent expansion of use beyond those authorized under law and described in this PIA?

Only approved FTC staff members have access to manage the FTC's Sprout Social accounts. Prior to beginning account administration, each staff member responsible for managing a social media account must sign and comply with the Commission's internal Rules of Behavior. The analytics report compiled by Sprout Social is internal and accessible to authorized FTC staff only.

The FTC's Sprout Social account is registered using official FTC email accounts. Administrators are not permitted to use personal accounts to manage FTC social media accounts. Furthermore, FTC staff are directed to use official government devices to manage accounts when possible. OPA staff may also use the agency's Twitter, Facebook and LinkedIn account credentials to access Sprout Social.

Finally, Sprout Social users can determine what additional personal information is made available to the public and the FTC, beyond the standard information required by Sprout Social to create an account, which is not available to the FTC, as noted earlier. Users can control whether their tweets and profiles are public or limited to only those they have previously approved of.

SECTION 5.0 - MAINTENANCE AND RETENTION OF PII

5.1 – How will the FTC maintain the PII, and for how long?

Any PII collected or maintained via Sprout Social will be retained and disposed of in accordance with applicable FTC policies and procedures and schedules issued or approved by the National Archives and Records Administration (NARA).

5.2 – Was the retention period established to minimize privacy risk?

Yes. Agency records schedules are required to maintain records only for as long as necessary to comply with Federal records preservation laws and guidance to prevent over-retention. In addition, per the FTC's own privacy policy, the FTC does not collect any unnecessary information, including PII. For engagement purposes on FTC's social networking Web sites, when required to preserve transcripts or other social media records, the FTC generally does not collect or maintain any PII beyond an account's handle or user name, which further minimizes potential privacy risks.

SECTION 6.0 – HOW THE AGENCY WILL SECURE PII

6.1 – Will the FTC's privacy and security officials coordinate to develop methods of securing PII?

Not applicable, to the extent that the FTC does not intend to routinely use Sprout Social to solicit, collect, maintain, or disseminate PII from members of the public. Sprout Social is used by the FTC to schedule its social media posts and collect general analytical reports such as the number of visitors to FTC social media pages, number of likes, retweets, shares, etc.

In those limited instances in which the FTC collects PII from a social media account through that account and/or through Sprout Social and incorporates that data into agency records and systems, FTC privacy and security officials coordinate to ensure that such records and systems are securely maintained and destroyed in accordance with a risk-based approach that takes into account the data's sensitivity and applicable threats and vulnerabilities in determining the appropriate security and privacy controls.

SECTION 7.0 – IDENTIFICATION AND MITIGATION OF OTHER PRIVACY RISKS

7.1 – What other privacy risks exist, and how will the agency mitigate those risks?

As noted earlier, the privacy risks are limited, since PII that may be collected by the FTC through Sprout Social from the FTC's social media accounts will ordinarily consist of public posting or comments, or in rare cases, private messages sent to the FTC. In addition, only public or aggregated analytics data about individuals is available to the FTC via Sprout, as already

discussed. Nonetheless, as explained earlier, the FTC limits access to the FTC's Sprout Social accounts to prevent the unauthorized collection of PII through these accounts.

As much as possible, the FTC uses Sprout to disseminate information that is already publicly available on the FTC websites; thus, consumers seeking access to FTC information are not required to visit the agency's page via Sprout Social or any of the other social media platforms where the FTC maintains a presence, if consumers are concerned about the privacy of these third-party platforms. If consumers want to avoid those platforms, comparable information is posted and available to users on the FTC's official website (www.ftc.gov).

The FTC routinely reviews Sprout Social's privacy policies for any changes that may affect the FTC's use of Sprout Social and will update its privacy policies as necessary to reflect any changes.

SECTION 8.0 – CREATION OR MODIFICATION OF A SYSTEM OF RECORDS

8.1 – Will the FTC's activities create or modify a "system of records" under the Privacy Act of 1974?

No. The FTC does not collect PII via Sprout Social in a manner that would require the FTC to create or modify a system of records under the Privacy Act of 1974. To the extent that any PII collected through Sprout Social from the FTC's social media accounts is incorporated into agency law enforcement files or other program records and maintained and retrieved by name or other personal identifier subject to the Privacy Act of 1974, no modification is necessary to the existing system of records or notice already published for that system. See FTC I-1, available at <https://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems>.