Social Media Monitoring

Product Overview and Features
Overview

Social Media Monitoring is part of Kroll’s non-credit suite of products. These products do not involve credit bureau data and provide services on information not tracked by credit bureaus.

Social Media Monitoring allows you to monitor multiple social media accounts and content feeds for privacy and reputational risks. You can set up monitoring for your Facebook, Twitter, LinkedIn and Instagram accounts to receive reports and alerts for content items such as image captions, posts, and comments.

You will be alerted to privacy risks like the exposure of personally identifying information, including:

- Phone number
- Email address
- Street address
- Date of birth
- Location data
- Credentials (username and password)
- Work history (employer name, current position, length of employment)
- Hometown
- Social Security number

Social Media Monitoring also searches for content that has the potential to create reputational risks, including:

- Vulgar language (curse words, profanity, or inappropriate slang)
- Drug and alcohol references,
- Discriminatory terms (words and phrases with racist, religious, and other bigotry type connotation)
- Harmful or threatening language (a user communicates about harming themselves or another)
- Sexual language

Product Details

Upon enrollment into a product configuration which includes Social Media Monitoring, a member will have the ability to link their eligible social media accounts to the monitoring service. After linking an account, the service generates a report that searches the past 45 days of historical information for alertable information and displays the results to the member. Once the account is linked, active monitoring is initiated and the member is notified of any subsequent alertable elements. Once active monitoring is initiated, the service scans each linked account daily.
Alert Types

**Privacy Alerts:** Social Media Monitoring Report – Facebook Privacy Alert Example:

![Facebook Privacy Alert Example](image)

The report will alert a subscriber of instances where they are sharing personal information to the public web, which can be used in a harmful manner by an identity thief. The alerts are generated from social profile details, as well as comments and wall posts which may have personal information in them.

**Reputation Alert:** Social Media Monitoring Report – Facebook Reputation Alert Example:

![Facebook Reputation Alert Example](image)

The service will also provide reputational risks which alert a subscriber of content that was found within their social network profiles and content feeds which may damage the subscriber’s reputation. This can include several different categories of potentially damaging content such as foul language, sexual content, and drug and alcohol references.

**Note:** Since the monitoring service is searching for content that matches a predetermined list of flagged content, there may be some content that the service does not capture. For example: colloquialisms, abbreviations, slang, and other terms that are not already in the predetermined list may not be captured. The predetermined list is updated but this does not guarantee that all reputational risks will be captured.
User Experience

This section identifies the common workflows for a user.

Social Media Monitoring Pop Up and Product Page

Upon initial login, the user will see a Pop Up on the Home page:

After the user closes the pop up window, they will select Social Media Monitoring from the dropdown:
The user will be redirected to the Social Media Monitoring Product Page:

**Linking Social Media Accounts**

The user will use the linking widget to link their social media accounts.
Linking Process Example 1 (Facebook):

After linking, the buttons shift over and are colored blue to signify successfully linked.
Linking Process Example 2 (Twitter)

Authorize IDShield Social Media Monitoring to use your account?

Sign In  Cancel

This application will be able to:
- Read Tweets from your timeline.
- See who you follow, and follow new people.
- Update your profile.
- Post Tweets for you.
- Access your direct messages.

Will not be able to:
- See your Twitter password.

Confirm Your Account

Testing Account

Confirm that this is the Twitter profile you want to monitor. If not, click Cancel and log out of Twitter.

Cancel  Confirm

You have successfully linked your Twitter profile. Your privacy and reputation will now be monitored.
Product Requirements

The following elements are required for user enrollment into Social Media Monitoring:

- Linking desired social media account with the Social Media Monitoring service
  - Requires logging into each account through the Social Media Monitoring website.
  - Please note that the monitoring service cannot link to accounts with Emoji’s in the user name.
- Enrollment profile data is utilized by the service to search for alertable privacy risks.

Social Media Monitoring Alerts

The member is notified of a new Social Media Monitoring Alert. The member logs into the member Portal and reviews the details of the alert.

  a. If the member deems the alert recognized and legitimate, use case ends.
  b. If a member acknowledges the alert and wants to take further action to resolve or understand the alert, the member may disassociate the information mentioned in the alert from their social media profile or contact a Kroll Fraud Investigator for advice regarding how to solve an issue.
  c. If the member is unable to resolve the issue by themselves or with the assistance of a Kroll Fraud Investigator, they can contact the relevant social media network for final remediation.

Restoration Process

The user should be able to resolve any issues that arise from the alerts by deleting or disassociating their accounts from their flagged content or by contacting the relevant social network for remediation. The member can contact a Kroll Fraud Investigator for advice regarding how to resolve the issue.

Monitoring Frequency

Social Media Monitoring is updated daily and alerts to the member are sent within 24-48 hours. Upon linking of each social media account, a baseline report is generated that searches historical data up to 45 days in the past for potential privacy and reputational risks. After linking, the monitoring service scans each profile daily for potential privacy and reputational risks. Due to LinkedIn’s Terms & Conditions, the user must relink Social Media Monitoring to LinkedIn every 45 days.
FAQs

Q: Does the Social Media Monitoring scan include content in private messages?
A: No, alerts are only for content that is displayed publicly. Private messages are not scanned.

Q: Does the Social Media Monitoring scan only content that I post, or does it include content that others post?
A: Social Media Monitoring reviews any content that you have added about yourself and public content associated with you. It will also return profile details about any other social network user that has publicly interacted with you on your Twitter, Instagram and LinkedIn profiles. Due to Facebook's terms of use, the monitoring application cannot provide alerts for anyone other than the person being monitored by the service.

Q: Is historical content included in my report?
A: Reports show the most recent 45 days of content items. Alerts generated for content that was last updated more than 45 days ago will be automatically deleted.

Q: How often is the Social Media Monitoring scan updated?
A: The service monitors the linked social media accounts on a daily basis and alerts will be sent within a 24-48 hour period after the content was added or updated to your social networks. LinkedIn is an exception to this; due to its current terms of use, your information cannot be automatically monitored and instead you will be required to accept the monitoring application for each new scan. Additionally, a LinkedIn profile can only be scanned every 45 days.

Q: How will I know my information is being monitored?
A: Each social media network requires your opt-in before monitoring can begin. When you click on the links to each social network, you will be provided with the steps necessary to authorize monitoring of your profile, updated feed and other content. Please note the service restrictions related to LinkedIn will require your authorization each time a scan is performed. You can cancel the monitoring service’s access to your social media accounts at any time.

Q: There are recent messages in my public content that I feel should have produced a reputational alert, but they didn’t. Why?
A: Social Media Monitoring searches for material that matches a predetermined list of content. Abbreviated or slang terms not on the predetermined list may not appear in your reports or alerts. While the list is updated regularly, it is possible that content that may be a reputational risk will not be captured.
**Tips to help Manage your Personal Reputation Online**

DO use the privacy and security features offered. Default settings generally do not offer a preferred level of privacy or security. Check settings periodically, as they can be reset if there is a change to the website.

DO share personal information sparingly. Social media sites may ask for a lot of information. Much of that information is used to make you more visible to acquaintances and those with shared interests. Think carefully about your use of the site – if you really only interact with close friends and family, you don’t have to include a lot of information to be “found.”

DO consider how your friends’ privacy settings might affect your privacy. If your posts show up in their profile, it’s possible they can be seen by others to whom you aren’t connected.

DO NOT post personally identifiable information (PII), information that is private to you and which could be used to locate or identify you as an individual, on social networking sites. For example, there should be no situation where you would need to post your SSN online.

DO NOT accept friend requests from strangers or post your location on social media, as this can increase your likelihood of becoming a victim of fraud.

DO NOT fall victim to the “nothing to hide” argument. Privacy in the digital age isn’t about hiding facts, it’s about protecting your personal information and your personal privacy. If you wouldn’t say it in public, don’t post it online.