Florida Schools Safety Portal & Social Media Monitoring

Shawna Reid & Jamie Braun
August 15, 2019

Florida Schools Safety Portal & Social Media Monitoring

- Required by Florida Statutes 1001.212(6)-(9)
- Through the collaboration and participation of:
  - Florida Dept. of Law Enforcement (FDLE)
  - Florida Dept. of Children and Families (DCF)
  - FivePoint Solutions
  - NTT Data Services
- Available to threat assessment teams for schools across the state of Florida to improve access to timely, complete and accurate information by authorizing school threat assessment teams to swiftly identify, assess and provide intervention services for individuals whose behavior may pose a threat to themselves or others.
Social Media Monitoring (SMM) Tool

- Allows school threat assessment teams to identify, assess and provide intervention services for individuals whose behavior may pose a threat to themselves or others
- Report suspicious activities to the proper authorities within the school district based on their Threat Assessment Plan

Features
- Real-time monitoring
- Customizable dashboards
- Unlimited keyword searches
- Geo-fencing
- Notifications configured at the state, district and school level
- Constantly expanding sites monitored

Examples of Social Media Sites Monitored
- Twitter
- Facebook
- Instagram
- YouTube
- Reddit
- Flickr
- Google+
- Pinterest

Other Examples Monitored
- Major news sites and local news
- Blogs: Millions
- Forums: Hundreds of thousands
- Customer review sites
- Regional and miscellaneous networks
Keywords & Geolocation

System includes keywords for the five topic types:
- Gun
- Bomb
- Bullying
- Mental Health
- General

Uses geo-tags defined at multiple levels depending on district population density.

System includes existing school specific data:
- When posts target a specific school, notifications are sent to that District/School
- Geo-fencing - geolocation data is provided by a social media platform to identify posts happening on or near the school

Identity Based Monitoring

<table>
<thead>
<tr>
<th>Status</th>
<th>Keyword</th>
<th>Location</th>
<th>Identity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Captured</td>
<td>Captured only if the name of the entity is named in the threat: “I’m going to hurt someone at Westfield High.”</td>
<td>Captured only if the threat is made when the individual is within the geo-fenced location on or near the school.</td>
<td>Individual’s handle is logged if threat is made on social media within defined geo-fence. Threats are then tracked from any location.</td>
</tr>
<tr>
<td>Not Captured</td>
<td>Not captured if no keywords show it is a threat against a specific school.</td>
<td>Not captured if threat is made from individual’s home.</td>
<td></td>
</tr>
</tbody>
</table>

When threats happen outside of the location and the profile is captured, then regardless of location all social chatter from this identity will be captured.
The new Florida Schools Safety Portal (FSSP) enacts the Marjory Stoneman Douglas Commission’s recommendation to improve access to timely, complete and accurate information by authorizing school threat assessment teams to swiftly identify, assess and provide intervention services for individuals whose behavior may pose a threat to themselves or others.

The FSSP will not be used to label students as potential threats, but rather is a tool to evaluate the seriousness of reported or identified threats and to assist in getting professional help when necessary.
Florida Schools Safety Portal (FSSP)

- Coordination with state agencies to provide a centralized integrated data repository with data analytics resources
- Improves access to timely, complete and accurate information
- Integrates data from:
  - Department of Education
  - Department of Children and Families
  - Department of Law Enforcement
  - Department of Juvenile Justice
  - Local law enforcement
  - Social Media
- Data includes:
  - School Environmental Safety Incident Reporting (SESIR) and discipline information.
  - FortifyFL, an application that shows suspicious activity reporting data.
  - Social Media Monitoring data, which searches social media posts containing certain keywords.
  - Baker Act Reporting Center data, which shows Baker Act proceedings were initiated under Florida’s Mental Health Act.
  - Law enforcement information; law enforcement officers will have access to law enforcement and juvenile justice records via links within the portal

Florida Schools Safety Portal (FSSP)

- The Florida Schools Safety Portal provides real-time access to information to quickly avert a reported or identified threat.
- Only users already authorized to access criminal justice data will be able to access the information via the portal.
- Information is temporarily displayed to authorized users for only 30 minutes and a screen timeout will immediately log inactive users out of the system.
- Authorized users will not be able to download or store information. The portal does not store information about students’ race, religion, disability or sexual orientation;
- Access to data is governed by applicable state and federal privacy laws.
- Threat assessment team members must undergo complete training and sign user agreements to obtain access to data.
Data Sources
Authorized users will access one system that will query from multiple data sources

- Florida Schools Safety Portal (FSSP)
- School Environmental Safety Incident Reporting Data (SESIR)
- FortifyFL (Suspicious Activity Reporting Data)
- Social Media Monitoring Data
- FDOE Law Enforcement Links
- DCF Baker Act Data

Disclaimer Statement
• Allows users the ability to perform searches against the data sources that are within the portal.
• Users with expertise or credentials in Law Enforcement will have access to law enforcement records through the available links.
• Users can access frequently asked questions as a general reference.
• Training Tutorials are readily available to users for review as needed.
Cybersecurity

- Strict data governance and security measures safeguard the protection of confidential education, health and law enforcement records, and ensures compliance with applicable state and federal privacy requirements in accordance with rules adopted by the respective source agencies.

- Every effort has been made to put proper preventative measures in place including security protocols and access controls to monitor and ensure data is protected.

- Web based training is required that includes topics on FSSP data security.

- Role based authentication is implemented so users are only authorized access to specific data.

- A disclaimer is displayed that must be accepted prior to final authentication into the FSSP dashboard.

What’s Next?

- Improving the availability of SESIR through more frequent collections. It is currently collected 3 times a year. A weekly collection is being considered.

- Working with other state agencies to identify and expand to additional data sources.

- The Behavioral Threat Assessment Instrument is currently paper based and will need to be digitized in order to integrate the tool into the FSSP.