



| Flash |

Residential Privacy Risks Amplified by High-Profile Incident

F-2025-04-15a

Classification: TLP:CLEAR

Criticality: Moderate

Intelligence Requirements: Executive Protection, Physical Security

April 15, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 11:56 AM (EDT) on April 14, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Residential Privacy Risks Amplified by High-Profile Incident

| Key Findings

- An April 13, 2025, attack on the official residence of Pennsylvania Governor Josh Shapiro underscores the continued risk residential exposures pose to public figures and executives. While Governor Shapiro was targeted in the official state residence rather than a private residence, the governor and his family were home at the time, and the incident highlights broader concerns around publicly accessible address information and the physical security of family dwellings. Personal addresses and home details are increasingly accessible online through public records, real estate listings, mapping services, and data aggregator sites, increasing high-profile individuals' risk of physical targeting.
- The suspect, identified as Cody A. Balmer, was arrested and charged with several felonies, including attempted homicide, terrorism, aggravated arson, and burglary. In interviews with police, Balmer acknowledged that he “harbored hatred” for Governor Shapiro and spoke of an obvious intent to hurt him physically.
- While current open source monitoring has not identified coordinated online threats following the incident, ZeroFox assesses that high-profile events of this

nature often trigger secondary risks, including digital harassment, doxxing, and opportunistic threat actor activity.

| Details

Although the incident appears isolated and no group has taken responsibility, this case does raise important executive protection issues.

- The suspect reportedly climbed through the perimeter of the fence and used makeshift incendiary devices. He confessed in interrogation that he would have inflicted physical harm had Governor Shapiro confronted him.¹
- Authorities have confirmed that the attack was not opportunistic and that it sprang from personal animosity, not ideological affiliation per se.²
- A surge in violent threats against politicians on both sides of the political spectrum in recent years has included the targeting of then-Speaker of the House Nancy Pelosi in 2022 (in which her husband Paul was violently attacked with a hammer), a plot to kidnap Michigan Gov. Gretchen Whitmer in 2023, and two assassination attempts against President Donald Trump during his second presidential campaign in 2024.³
- In contrast to other recent high-profile incidents targeting public figures and executives, no significant surge in online support, glorification of the attack, or amplification has yet been observed, but the online reaction to such events often evolves over time.

¹

[hXXps://apnews\[.\]com/article/josh-shapiro-arson-police-fire-pennsylvania-governor-2d17ec60c48f7d4d15123dda60c88699](https://apnews.com/article/josh-shapiro-arson-police-fire-pennsylvania-governor-2d17ec60c48f7d4d15123dda60c88699)

²

[hXXps://www.cbsnews\[.\]com/philadelphia/news/cody-balmer-governors-residence-fire-josh-shapiro-harrisburg/](https://www.cbsnews.com/philadelphia/news/cody-balmer-governors-residence-fire-josh-shapiro-harrisburg/)

³

[hXXps://www.cnn\[.\]com/2025/04/14/us/pennsylvania-governor-arson-what-we-know-hnk/index.html](https://www.cnn.com/2025/04/14/us/pennsylvania-governor-arson-what-we-know-hnk/index.html)

- Such incidents often stoke heightened fears about the visibility of high-profile individuals' homes and serve as reminders of the downstream risks of such information being publicly available, including targeted harassment, impersonation, or opportunistic cyber activity.

| Analyst Commentary

ZeroFox assesses that residential privacy and removal of personal information from online sources are ongoing critical components of any modern executive protection strategy. This attack does not reflect a coordinated campaign or broader activist sentiment but reinforces several trends observed in past cases:

- Attacks may stem from personal grievances or perceived injustice versus being tied to a specific ideological affiliation.
- Known official and private residential addresses (visible through data aggregator sites), mandated property record disclosures, and real estate listings continue to present risk vectors that may be exploited in both physical and digital threats.
- The absence of immediate online threats does not eliminate risk; threat activity commonly escalates in the days or weeks following a high-profile event.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%