

Police Department (OSUPD). At OSUPD, I served initially as a patrol officer before moving to the Investigative Services Division, where I served as the department's computer crime investigator for approximately six years. While a detective with OSUPD, I also served as a Special Deputy United States Marshal on the Federal Bureau of Investigation's Cybercrime Taskforce from 2005-2007. Except for a period from May 2008 until approximately May 2009 (while in private employment) I have been a law enforcement officer since 1999. In that time, I have held commissions with the Ohio State University Police Department, the Worthington, Ohio, Division of Police, and the Ohio Bureau of Criminal Investigation. I held my federal commission as a Special Deputy United States Marshal for the FBI's cybercrime taskforce from 2005-2007.

3. During my time in law enforcement, I have investigated hundreds of criminal offenses, including countless computer-connected criminal events, and have obtained and numerous search warrants. Many of the search warrants I have obtained and executed relate to electronic devices and the data stored therein.

INFORMATION SOUGHT AND LEGAL BASES THEREFORE

4. This application seeks a search warrant for records held by ADT, LLC, ("ADT") which accepts legal process in Ohio c/o CT Corporation System, Easton Way, Ste 125, Columbus, Ohio. ADT offers to the public various items of hardware (such as internet-enabled wireless surveillance cameras) as well as software applications with which customers can view, record, and store footage via the internet through a connection to the ADT computer servers. The contents of videos, if stored, are sent online to ADT by electronic communication to the company and saved on ADT's computer systems for users. ADT allows users of its service to create accounts, associated with email addresses, to control access to a user's account for storing and viewing recorded video. ADT's application is available on various internet-enabled smartphones, such as the Apple iPhone. ADT therefore satisfies the definition of a "remote computing service" under 18 U.S.C. § 2711(2) because it "provi[des] to the public...computer storage or processing services by means of an electronic communications system."

5. Because of the services ADT provides, it is bound by the terms of the federal Stored Communications Act. The federal Stored Communications Act, 18 U.S.C. § 2701 et seq., controls the access of records, content, and other information from electronic communication service providers and remote computing service providers by governmental entities. 18 U.S.C. § 2703(a) states, in part:

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant...in the case of a State court, issued using State warrant procedures...by a court of competent jurisdiction.

6. 18 U.S.C. § 2703(b) states, in part:

A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication...without required notice to the subscriber or customer, if the governmental entity obtains a warrant...issued using State warrant...by a court of competent jurisdiction.

7. 18 U.S.C. § 2703(c) states, in part:

A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity...obtains a warrant...issued using State warrant procedures...by a court of competent jurisdiction.

8. Ohio Courts of Common Pleas satisfy the federal statutory definition of a “court of competent jurisdiction” under 18 U.S.C. § 2711(3)(B) (“a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants”).

Based on the foregoing facts, Affiant believes that the records kept by ADT for the accounts identified above may contain content, activity logs, personal identifiers, and other information that is relevant to this ongoing investigation, including but not limited to the following for the timeframe from 1600 hrs – 1700 hrs EDT (UTC-4) on April 20, 2021:

- **Subscriber Information:** Basic subscriber information for the above-identified accounts consisting of account creation date(s), activation information, any and all email address(es), telephone numbers, or other contact information associated with the account(s);
- **Non-content:** Including but not limited to access logs, including deletion logs, showing dates and times the account has been accessed (or attempted

to be accessed), metadata of such access or attempt (including IP addresses, device information, device name cookie information, etc.), timestamps and IP address(es) for the account logins/logouts, and any other accounts associated by cookie information stored in connection therewith; and

- **Content:** Any and all content data, including but not limited to video, audio, pictures, and communications (including any service communications with ADT, LLC);

9. 18 U.S.C. § 2703(g) does not require the presence of an officer for service or execution of search warrants issued under that chapter that are seeking the disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

FACTS ESTABLISHING PROBABLE CAUSE

10. On April 20, 2021, Officers from the Columbus Division of Police responded to the area of 3171 Legion Lane, Columbus, Ohio on a reported disturbance. Shortly after arrival, one officer intervened in a physical altercation occurring between people at that scene. In the course of events, the officer fired his duty weapon at one of the participants in the altercation, resulting in that person's death. During the course of the subsequent investigation, at least one camera operating through the ADT, LLC company was found at the residence.

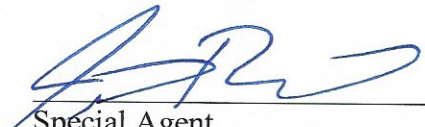
11. A resident of the address was interviewed and revealed that she had an application on her cellular telephone allowing her to access the ADT account. The account identifiers listed above were obtained from that application.

12. It is believed that ADT allows users to store copies of videos on servers under its control. Additionally, access logs may verify whether anyone accessed the account to delete any account data. Other information may verify ownership and/or account usage.

13. On April 21, 2021, the ADT, LLC account that is the target of this investigation was preserved, and ADT, LLC acknowledged its preservation obligations.

14. Taking all of these factors into consideration, probable cause exists for this Court to issue a search warrant for the entirety of the ADT account associated with the identifiers listed above for the specific categories of data listed above for the specific timeframe listed above. Affiant therefore requests that this Court issue a search warrant allowing investigators to obtain the video, information, and records sought from ADT in connection with that account.

Further Affiant sayeth naught.



Special Agent
The Ohio Bureau of Criminal Investigation

Sworn to and subscribed before me this 2nd day of June, 2021 at 1:47 am/pm.



Honorable Judge
Franklin County Court of Common Pleas