UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

In the Matter of the Search of

All contents and electronically stored information within the following property, all currently located at the Sioux Falls HSI office:

Verizon Samsung Galaxy S5
Model SM-G900V
IMEI: 990004915668275

and

T-Mobile Samsung
Model SGH-T469
IMEI: 354419034824924
S/N: RQ6Z434738R

No. 14-MC-97

APPLICATION FOR SEARCH AND SEIZURE WARRANT

I, Craig Scherer, being duly sworn depose and say:

I am a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) in Sioux Falls, South Dakota, and have reason to believe that all contents and electronically stored information within the following property, all currently located at the Sioux Falls, South Dakota HSI office:

Verizon Samsung
Model SM-G900V
IMEI: 990004915668275

and

T-Mobile Samsung
Model SGH-T469
IMEI: 354419034824924
S/N: RQ6Z434738R.

there is now concealed certain property, namely: that fully described in Attachment A hereto, which I believe is property constituting evidence of the commission of criminal offenses, contraband, the fruits of crime, or things otherwise criminally possessed, or property designed or intended for use or which is or has been used as the means of committing criminal offenses, concerning violations of 21 U.S.C. §§ 841(a)(1) and 846 and 18 U.S.C. § 1956.

The facts to support a finding of Probable Cause are contained in my Affidavit filed herewith.

Special Agent Craig Scherer
U.S. Department of Homeland Security
Immigration and Customs Enforcement

Sworn to before me, and subscribed in my presence on the 11 day of September, 2014, at Sioux Falls, South Dakota.

JOHN E. SIMKO
United States Magistrate Judge

ATTACHMENT A

1. All records on the devices described in the heading of the document to which this attachment is attached that relate to violations of 21 U.S.C. §§ 841 and 846 and 18 U.S.C. § 1956, including:

    a) lists of customers and contacts and related identifying information;

    b) types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

    c) any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

    d) any information recording schedule or travel;

    e) all bank records, checks, credit card bills, account information, and other financial records;

    f) Information pertaining to assets owned or under the control of the owners of the devices being searched, including but not limited to Vehicle Identification Numbers (VINs), serial numbers and/or other identification numbers of assets;

    g) Photographs and/or videos, in particular, photographs and/or videos of co-conspirators, assets, and for controlled substances.

2. Evidence of user attribution showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

IN RE ORDER REQUIRING GOOGLE, INC. TO ASSIST IN THE EXECUTION OF A SEARCH WARRANT ISSUED BY THIS COURT

Case No. 14-MC-97

APPLICATION

INTRODUCTION

The United States of America, by and through Brendan V. Johnson, United States Attorney, and Jennifer D. Mammenga, Special Assistant United States Attorney, hereby moves this Court under the All Writs Act, 28 U.S.C. § 1651, for an order requiring Google, Inc. ("Google") to assist in the execution of a federal search warrant by bypassing the lock screen of an Android device, specifically, a Samsung Model SM-G900V Galaxy S5, SKU: SMG900VZWV, FCC ID: A3LSMG900G and IMEI: 990004915668275 on the Verizon Network.

FACTS

The Department of Homeland Security currently has in its possession an Android device that was seized pursuant to a search warrant issued by this Court. Initial inspection of the Android device reveals that it is locked. Because the Android device is locked, law enforcement agents are not able to examine the data stored on the Android device as commanded by the search warrant.

Google, the creator of the Android operating system and producer of the Android device, may have the capability of bypassing the Android device's lock

and thereby retrieving data stored on the Android device that is not currently accessible to the Department of Homeland Security. This Application seeks an order requiring Google to use any such capability, so as to assist agents in complying with the search warrant.

The United States requests that the Court order that Google, if necessary, must reactivate the Google account associated with the Android Device for the limited purpose of complying with the search warrant.

Further, the United States requests that Google be directed to: (1) provide a single password reset for the Android device; (2) provide the new password to the law enforcement officer executing the search warrant; and (3) upon unlocking the target Android device, again reset the Google account password promptly upon notice that the imaging of the phone is complete, without providing it to the law enforcement officer or agency so as to prevent future access.

Further, the United States represents that the reset process may not be unobtrusive to the subject and that the subject may receive notice to one or more accounts of the reset. Accordingly, the United States requests that the Court order that any such notice is not a violation of any seal or nondisclosure requirement.

Finally, the United States does not seek authority to use the new password to attempt to access the subject's online accounts other than as synchronized on, and stored in, memory within the target device at the time of

execution of the warrant, and does not object to the Court prohibiting such use of the password to be provided by Google.

DISCUSSION

The All Writs Act provides that "[t]he Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). As the Supreme Court explained, "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute." *Pennsylvania Bureau of Correction v. United States Marshals Service,* 474 U.S. 34, 43 (1985). "The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice... and encompasses even those who have not taken any affirmative action to hinder justice." *United States v. New York Tel. Co.,* 434 U.S. 159, 174 (1977). Specifically, in *United States v. New York Tel. Co.,* the Supreme Court held that the All Writs Act permitted district courts to order a telephone company to effectuate a search warrant by installing a pen register. Under the reasoning of *New York Tel. Co.*, this Court has the authority to order Google to use any capabilities it may have to assist in effectuating the search warrant for the Android device by unlocking the Android Device.

The government is aware, and can represent, that in other cases, courts have ordered Google to assist in effectuating a search warrant by unlocking

other Android devices under the authority of the All Writs Act. Additionally, Google has complied with such orders.

The requested order would enable agents to comply with this Court's warrant commanding that the Android device be examined for evidence identified by the warrant. Examining the Android device without Google's assistance, if it is possible at all, would require significant resources and may harm the Android device. Moreover, the order is not likely to place any unreasonable burden on Google.

Respectfully submitted this 11th day of September, 2014.

BRENDAN V. JOHNSON
United States Attorney

JENNIFER D. MAMMENGA
Special Assistant United States Attorney
P.O. Box 2638
Sioux Falls, SD 57101-2638
Telephone: (605) 357-2361
Facsimile: (605) 330-4410
E-Mail: jennifer.mammenga@usdoj.gov

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
SOUTHERN DIVISION

IN RE ORDER REQUIRING GOOGLE, INC. TO ASSIST IN THE EXECUTION OF A SEARCH WARRANT ISSUED BY THIS COURT

Case No. 14-MC-97

ORDER

Before the Court is the Government's motion for an order requiring Google, Inc. ("Google") and Verizon to assist law enforcement agents in the search of an Android Device. Upon consideration of the motion, and for the reasons stated therein, it is hereby

ORDERED that Google assist law enforcement agents in the examination of a Samsung Model SM-G900V Galaxy S5, SKU: SMG900VZWV, FCC ID: A3LSMG900G and IMEI: 990004915668275 on the Verizon Network (the "Android Device"), acting in support of a search warrant issued separately by this Court;

FURTHER ORDERED that Google shall, if necessary, reactivate the Google account associated with the Android Device;

FURTHER ORDERED that Verizon provide a temporary data connection, if necessary, for the identified device so Google can comply with the search warrant and this Court's order.

FURTHER ORDERED that Google shall: (1) provide a single password reset for the mobile device; (2) provide the new password to the law enforcement officer executing the search warrant; and (3) upon unlocking the

target mobile device, again reset the Google account password promptly upon notice that the imaging of the phone is complete, without providing it to the law enforcement officer or agency so as to prevent future access;

FURTHER ORDERED that the reset process need not be unobtrusive to the subject, the subject may receive notice to one or more accounts of the reset, and such notice is not a violation of any seal or nondisclosure requirement;

FURTHER ORDERED that the law enforcement agent executing the search warrant is prohibited from using or attempting to use the new password to attempt to access the subject's online accounts other than as synchronized on and stored in memory within the target device at the time of execution of the warrant.

Dated: Sept 11, 2014

BY THE COURT:

JOHN E. SIMKO
United States Magistrate Judge