Second Transparency Report

SharpSpring Technologies

TRANSPARENCY REPORT ON GOVERNMENT AND LAW ENFORCEMENT REQUESTS FOR USER INFORMATION

Covering the Period of: 06, 2020—12, 2020

Date Published: 01/01/2021

INTRODUCTION

SharpSpring is pleased to release our second transparency report covering the second half of 2020.

ABOUT OUR TRANSPARENCY REPORT

Like many other technology companies, we sometimes receive requests from law enforcement agencies in both the United States and abroad who seek information about our users relating to criminal [and civil/intelligence/law enforcement...] investigations. We have a legal obligation to respond to valid government requests for user data. Similarly, we believe that we have a duty to inform our users and the public at large about those requests, and that is why we have prepared this transparency report.

Protecting our users' privacy is very important to us .For that reason, we carefully review each request for user data, and work with law enforcement to narrow such requests where possible. Our aim is to fully meet our legal obligations while honoring the trust that our users place in us and our services.

This transparency report provides information relating to law enforcement requests for user data that we processed between July 01, 2020 and Dec 30, 2020.

REPORT SUMMARY

During this period we received a total of 0 requests for user information from U.S. law enforcement agencies. This is neither an increase, nor decrease from the 0 requests we processed in the past. This is in part attributable to this being our second official public report and not ever having received requests for user information.

ADDITIONAL FEATURES

MLAT Requests

A Mutual Legal Assistance Treaty (MLAT) is a treaty between the U.S. and another country that establishes a process for the two country to assist each other in criminal investigations. The MLAT process provides a way for foreign governments to ask the U.S. government to issue a

request for user information. Requests that comes through the MLAT process sometimes say so, but often they appear to be identical to any domestic request for information. In this reporting period 0% of the search warrants and 0% of court orders we received were explicitly identified as having been issued through MLAT procedures. These requests came from 0 different countries.

All Writs Act

The All Writs Act is a federal law from 1789 under which courts can authorize orders ("writs") that compel a party to take a particular action. Following the December 2015 San Bernardino shooting, the U.S. government attempted to use the All Writs Act to compel Apple to circumvent the encryption of an iPhone seized during the investigation, resulting in increased public interest in requests made under this law. During the period of July 2020 - Dec 2020 we have not received any orders under the All Writs Act of 1789.

HOW TO READ THIS REPORT

General Approach

Throughout this report we generally adopt the definitions and best practices described in the*Transparency Reporting Toolkit's Reporting Guide and Template* created by the Open Technology Institute at New America and the Berkman Klein Center for Internet & Society at Harvard University. We make every effort to note where our definitions or approach is different than those in the Toolkit.

Services Covered

SharpSpring offers many different products and services, including:

- Customer Relationship Manager
- Social Tools
- Email Marketing
- Marketing Automation
- Site Tracking
- Ad Bidding

This transparency report covers all of these products and services.

Important Company Practices

In responding to requests we make several important determinations to ensure that we fully comply with lawful requests while respecting the privacy of our users. These decisions include:

- **Reasons for rejecting requests:** We review all government requests carefully. There are many reasons why we may conclude that a request is deficient and should be rejected. These may include:
    - Lack of information
    - Invalid Requests
- **Counting Selectors:** At several points in this report we talk about the number of "selectors" in a request. A selector may simply be an identifier (e.g. a username, IP address, e-mail address, phone number, etc.) specified by law enforcement in a legal process when requesting user information. When counting the number of selectors, we classify each request accordingly and count the amount of selectors for the request and how many accounts in total are affected.

INTERNATIONAL REQUESTS

Although SharpSpring is a U.S. company, we have a corporate presence in several other countries. Because of that, we respond to requests in all countries that have legal jurisdiction over our operations. When we receive requests from non-US governments we log the request, work with local counsel to validate the request, respond and then categorize and log the outcome.

ACKNOWLEDGMENTS

This transparency report is based on the *Transparency Reporting Toolkit's Reporting Guide and Template* created by the Open Technology Institute at New America and the Berkman Klein Center for Internet & Society at Harvard University. For more information about transparency reporting and the process of creating a transparency report, you can read the entire Toolkit at: HYPERLINK "https://www.newamerica.org/oti/transparency-toolkit/" https://www.newamerica. HYPERLINK "https://www.newamerica.org/oti/transparency-toolkit/" org/oti/transparency-toolkit/.

UNITED STATES REQUESTS

TYPES OF LEGAL PROCESSES RECEIVED

	Search Warrants	Wiretap Orders	Pen Register / Trap and Trace Orders	Other Court Orders	Subpoenas Criminal	Subpoenas Civil	Emergency Requests	TOTAL
# Received (1*)	0	0	0	0	0	0	0	0

SELECTORS & ACCOUNTS FOR ALL OF THE ABOVE REQUEST

Total # of Selectors Specified by All of the Above Requests	0

Total # of Accounts Potentially Affected by All of the Above Requests	0

PRESERVATION REQUESTS

# Received	# of Selectors Specified	# of Accounts Responsive
0	0	0

USER NOTIFICATION (PRE-DISCLOSURE)

	Requests with Non-Disclosure Orders	No Non-Disclosure Order, Notice was provided	No Non-Disclosure Order, Notice was not Provided	Total
# Received	0	0	0	0
% of Total	0	0	0	100%

(1) Total number of orders of any kind acted on (e.g., rejected or responded to) during second half of 2020.*

OUTCOMES / COMPLIANCE WITH REQUESTS

SEARCH WARRANTS	**Rejected**	**No Data**	**Content Disclosed**	**Only Non-Content Disclosed**	**TOTAL**
#of Requests	0	0	0	0	0
% of Total	0	0	0	0	100%

WIRETAP ORDERS	**Rejected**	**No Data**	**Content Disclosed**	**Only Non-Content Disclosed**	**TOTAL**
#of Requests	0	0	0	0	0
% of Total	0	0	0	0	100%

PEN REGISTER ORDERS	**Rejected**	**No Data**	**Content Disclosed**	**Only Non-Content Disclosed**	**TOTAL**
#of Requests	0	0	0	0	0
% of Total	0	0	0	0	100%

OTHER COURT ORDERS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests	0	0	0	0	0
% of Total	0	0	0	0	100%

CRIMINAL SUBPOENAS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests	0	0	0	0	0
% of Total	0	0	0	0	100%

GOVT. CIVIL SUBPOENAS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests	0	0	0	0	0
% of Total	0	0	0	0	100%

EMERGENCY REQUESTS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests	0		0	0	0
% of Total	0	0	0	0	100%

TOTAL—ALL ORDERS	Rejected	No Data	Content Disclosed	Only Non-Content Disclosed	TOTAL
#of Requests	0	0	0	0	0
% of Total	0	0	0	0	100%

NATIONAL SECURITY REQUESTS

Option #3 Bands of 250 (semiannually)	National Security Letters + FISA Orders for Content + FISA Orders for Non-Content
# Received	0
# of Customer Selectors Targeted	0
# of Accounts Responsive	0

> “(1*) Orders for pen register and trap and trace surveillance.
> *(2*)* Orders for production of business records, not counting orders for ongoing disclosure of call detail records.
> *(3*)* Orders for production of call detail records. ”

INTERNATIONAL REQUESTS

TYPES OF LEGAL PROCESSES RECEIVED

	Retrospective1	Prospective 2	TOTAL

# Received(3*)	0	0	0

SELECTORS & ACCOUNTS FOR ALL OF THE ABOVE REQUESTS

Total # of Selectors Specified by All of the Above Requests	0

Total # of Accounts Potentially Affected by All of the Above Requests	0

USER NOTIFICATION

	Requests with Non-Disclosure Orders	**No Non-Disclosure Order, Notice was Provided**	**No Non-Disclosure Order, Notice was not provided**	**TOTAL**
# Received	0	0	0	0
% of Total	0	0	0	100%

"(1*) For existing, historical user data.
(2)* For data that will be collected in the future.
(3)* Total number of orders of any kind acted on (e.g., rejected or responded to) during [TIME PERIOD]."

OUTCOMES / COMPLIANCE WITH REQUESTS

	Rejected	**No Data**	**Content Disclosed**	**Non-Content Disclosed**	**TOTAL**
# Received	0	0	0	0	0
% of Total	0	0	0	0	100%

GLOSSARY / DEFINITIONS

These definitions are an amalgamation of existing transparency report glossaries and encompass the best practices in defining legal processes as identified in*Transparency Reporting Toolkit Memo 2: Defining Legal Processes*.

U.S. LEGAL PROCESSES TERMS

2703(d) Court Orders

Often known as a "d order" or ECPA order, § 2703(d) court orders are granted based on an intermediate standard that is less stringent than the probable cause standard for warrants, but more demanding than the mere relevance standard required for subpoenas. To receive an ECPA court order, a law enforcement agency must present specific and articulable facts to a judge or magistrate demonstrating that there are reasonable grounds to believe the requested information is relevant and material to an ongoing criminal investigation. The orders compel an internet service provider to disclose more information than is usually obtainable by subpoena, like records relating to a subscriber other than the contents of communications. This could include the IP address associated with a particular email sent from that account or used to change the account password (with dates and times) and the non-content portion of email headers such as the "from," "to" and "date" fields. An ECPA court order is available only for criminal investigations.

Other Court Orders

Other court orders refers to valid and binding orders issued by local, state, or federal courts, other than the court orders counted separately (e.g., search warrants, pen register and trap and trace orders, etc.). Such orders generally seek historical information and more detailed information than is available using a subpoena. To obtain a court order, a judge must sign the order indicating that the law enforcement entity seeking the court order has made the requisite showing under the law to obtain the order.

Emergency Request/Disclosure

Also referred to as exigent requests or emergency disclosures, these are voluntary disclosures made to a government agency seeking information to save the life of a person who is in peril or prevent serious physical injury. These disclosures are made when the company has reason to believe that doing so is necessary to prevent death or serious physical harm to someone.

Emergency requests must contain a description of the emergency and an explanation of how the information requested might prevent the harm. The information provided in response to an emergency request is limited to what the company believes would help prevent the harm. Examples of situations where emergency requests might be necessary would include kidnappings, missing person cases, attempted suicides, etc.

Search Warrant

Also known as probable cause court orders or warrants, a search warrant is a court order granted based on a showing of probable cause, the highest standard to obtain evidence. To successfully receive a warrant, government agencies are required to provide evidence of "reasonable ground to suspect that a person has committed or is committing a crime, or that a place contains specific items connected with a crime." The order must be supported by sworn testimony and sufficient evidence, and must specifically identify the place to be searched and the items to be seized. Except in emergency circumstances, a search warrant is required before the company will disclose stored content (e.g., documents, photos, e-mails and voice messages).

Subpoena

A subpoena is a legal demand issued directly by a prosecutor or a law enforcement or administrative agency to a company, usually without prior court approval. A prosecutor or agency can issue a subpoena when they determine that the material sought is relevant to a civil or criminal investigation. Of all of the types of legal process, subpoenas require the lowest standard of proof. However, subpoena can only be used to compel disclosure of non-content information— for example, basic subscriber information, name and address, IP address, call records, or sign-in and sign-out records.

Pen Register/Trap and Trace Order (PRTT)

PRTT orders are court-issued orders used to authorize the real-time, prospective collection of non-content dialing or addressing information (sometimes called "metadata") about the incoming and outgoing communications of a target in real time. Such information may include phone numbers, email addresses, IM handles, IP addresses, and the domain name of web sites visited (i.e., everything before the / in the web address), as well as time stamps and the size or length of the communication. Trap and trace orders apply to information about incoming communications while pen registers apply to information about outgoing communications, and the two orders are usually issued in combination. It's easier for a government agency to get a PRTT order than wiretap order or search warrant. Rather than presenting facts that demonstrate probable cause, they need only certify that information likely to be obtained will be relevant to an ongoing criminal investigation. PRTTs typically last 60 days, and can be renewed for additional 60 day periods. Unlike with wiretaps, there is no requirement that the user be notified after the surveillance is completed.

Wiretap Order

A wiretap order is judge-issued order that requires a wire or electronic communications provider to provide to law enforcement real-time access to the content of communications. The order can relate to the content of telephone or internet communications. When compared to other kinds of legal process, wiretap orders are the most difficult for law enforcement to obtain. In order to obtain a wiretap order, a government agency must demonstrate probable cause that:

someone is committing one of certain offenses specified in the Wiretap Act, b) the wiretap will collect information about that crime, and c) the crime involves the telephone number or account that will be tapped. Before issuing the wiretap order, the court must also find that other, less intrusive investigatory techniques have failed (or probably would fail), or are too dangerous to attempt. Wiretap orders run for 30 days (which can be renewed) and the court must generally notify the subjects of wiretap orders with a reasonable time after the conclusion of the wiretap.

NATIONAL SECURITY TERMS

Foreign Intelligence Surveillance Court (FISC) Order

Also knows as FISA requests or FISA orders, Foreign Intelligence Surveillance Court orders are secret demands that can require U.S. companies to hand over or assist in the monitoring of users' communications content and non-content data. The Foreign Intelligence Surveillance Act (FISA) is a U.S. law, originally enacted in 1978, to govern how the U.S. government collects foreign intelligence for national security. As with the regular court system in regular criminal investigations, the FISA-created Foreign Intelligence Surveillance Court can issue wiretap (or "electronic surveillance") orders, search warrants, PRTT orders, and orders for non-content records ("Section 215 orders"). However, unlike in the regular court system, FISC orders do not require probable cause of a crime, and all FISC orders are accompanied by an indefinite gag order (although companies are now allowed under the USA FREEDOM Act of 2015 to report aggregate data about the FISC orders they receive). In addition to providing for individualized surveillance demands as in criminal cases, FISA—as amended by the FISA Amendments Act of 2008—also allows for the issuance of non-individualized surveillance orders authorizing broad programs of surveillance that can target any person outside of the U.S., including their communications with people inside the U.S., so long as those communications are believed to have foreign intelligence value. In these cases, the court does not approve specific targets, but instead approves the government's own guidelines for how it picks its targets and minimizes non-pertinent data.

National Security Letter

Also known as national security demands or national security requests, national security letters (NSL) are secret subpoenas issued by the Federal Bureau of Investigations under 18 U.S.C. §2709, a part of the Electronic Communications Privacy Act (ECPA). In order to obtain an NSL,

the Director of the FBI or a senior FBI designee or the special agent in charge of a local FBI field office must provide a written certification that demonstrates the information requested is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. NSLs can only be used to obtain non-content, like certain basic subscriber and transactional information. Companies can only disclose the receipt of NSLs in aggregate amounts, as described in the USA Freedom Act.

NON-U.S. LEGAL PROCESS TERMS

Prospective Order

An order for the real-time collection of information that will be generated in the future, such as the content and metadata associated with phone calls and e-mails that the target will send during the period in which the order is active.

Retrospective Order

An order for the collection of information that a company already has about and from the target, such as the content and metadata associated with phone calls and e-mails that the target sent using the systems owned by the company receiving the order.

SOURCES OF LAW

Electronic Communications Privacy Act (ECPA)

The Electronic Communications Privacy Act is a United States federal statute that prohibits a third party from intercepting or disclosing communications without authorization. The Act, which was originally passed as an amendment to the Wiretap Act of 1968, applies to both government employees and private citizens. It protects communications in storage as well as in transit.

The Act consists of three parts. The first, often referred to as “the Wiretap Act” or “Title III,” outlaws the unauthorized interception of wire, oral, or electronic communications and establishes a judicial supervised procedure to permit such interceptions for law enforcement purposes. The second, the Stored Communications Act (SCA), focuses on the privacy of, and government access to, stored electronic communications. The third, typically referred to as “the Pen Register Statute,” creates a procedure for governmental installation and use of pen registers as well as trap and trace devices. It also outlaws such installation or use except for law enforcement and foreign intelligence investigations.

Foreign Intelligence Surveillance Act (FISA)

The Foreign Intelligence Surveillance Act is a U.S. law, originally enacted in 1978 to govern how the U.S. government collects foreign intelligence for national security. This Act created the Foreign Intelligence Surveillance Court, which consists of 11 federal district court judges who review government applications for electronic surveillance and other types of intelligence collection. The FISA Amendments Act, passed in 2008, enables the court to require U.S. companies to provide information and the content of communications associated with the accounts of non-U.S. citizens or non-lawful permanent residents who are located outside the United States, as well as certain U.S. persons, subject to certain limitations. The DOJ oversees the agencies involved in carrying out FISA-authorized activities. FISA requires these agencies to brief Congress on a regular basis and present all pertinent FISA court documents.

Pen Register Statute

The federal criminal pen register statute was enacted in 1986 as part of ECPA to govern real-time

interception of telephone numbers dialed or transmitted. The statute establishes the process for obtaining pen register and trap and trace orders. In 1998, Congress amended FISA to authorize the government to use pen registers to collect foreign intelligence information in national security investigations after obtaining an order from the Foreign Intelligence Surveillance Court.

Stored Communications Act (SCA)

The Stored Wire and Electronic Communications and Transactional Records Access, commonly referred to as the Stored Communications Act, was enacted in 1986 as part of the Electronic Communications Privacy Act. The Act addresses voluntary and compelled disclosure of stored communications held by third-party internet service providers.

The Act distinguishes between privacy protections for two types of network service providers: electronic communication service providers and commercial service providers. The statute creates two kinds of protections for customers. First, the Act enacts a broad prohibition against providers voluntarily sharing customers’ communications with the government or others, subject to certain enumerated exceptions. Second, it outlines procedures permitting the government

to require the disclosure of customers’ communications or records. The statute applies to both content and non-content information.

Wiretap Act

Also known as Title III, the Wiretap Act was enacted in 1968 as part of the Omnibus Crime Control and Safe Streets Act of 1968. The Act provides protection against intentional and non-consensual interception of electronic communications, establishes procedures for the government to

obtain warrants to authorize wiretapping, and regulates the disclosure and use of authorized intercepted communications by investigative officers. The Act imposes a stringent warrant requirement before investigators can obtain a wiretap order.

OTHER TERMS USED

Accounts Responsive

This term describes the number of accounts that are responsive to a government request for information. These are the accounts that satisfy the elements of the government request after the company searches their records using the various selectors specified by law enforcement in the legal process (i.e. username, IP address, e-mail address, phone number, etc.). An individual may have multiple accounts, or a single account may be used by many people; the number of accounts responsive is only a rough proxy for the number of impacted individuals.

Selectors Specified

Also referred to as account identifiers or users/accounts specified, selectors specified refers to the number of identifiers (i.e. username, IP address, e-mail address, phone number, etc.) specified by law enforcement in legal process when requesting user information. Some legal processes may include more than one identifier, and multiple identifiers may be used to try to identify a single account.

Process Received

Process received describes the individual requests for information that an internet or telecommunications company has received. In transparency reports, companies disclose the specific number of each type of legal process received. These include search warrants, subpoenas, 2703(d) orders, emergency requests, wiretap orders, and pen register orders.

Non-Disclosure Order

A company may be prohibited from notifying users about a legal request for their information for some period of time. These prohibitions may take the form of a statute, court order, or some other limitation that prevents the company from providing notice to the user prior to complying with the request for information.

Content

Content refers to the information concerning the substance, purport, or meaning of a particular communication, which can include the text of e-mails, text messages, direct messages, Tweets, videos, and more. Obtaining content generally requires law enforcement to secure a warrant.

GLOSSARY / DEFINITIONS (CONTINUED)

What is considered content can be platform and service dependent and may be subject to disagreement between law enforcement and companies.

Non-Content

Non-content user information includes any and all account information that is not considered to be content. This can include basic subscriber information such as the name used to create an account, the IP address from which an account was created, or the IP address used to sign in to an account, along with dates and times. Non-content information can also include more detailed transactional data about a user's communications such as the IP addresses, email addresses, IM handles, or phone numbers that sent or received the communications, as well as when the communications occurred, how long in duration, and how large in size they were. The legal standard that law enforcement must meet depends on the exact kind of information they seek to obtain (see section on U.S. Legal Process Terms).

Request Rejected

A request is considered to be rejected when a company denies a request in full, providing neither non-content nor content information about the specified account or accounts. Companies generally reject requests due to some defect in the request, such as invalid process, the request is served on the wrong company, the request fails to specify an account, or it was duplicative of a previous request. A request can also be considered rejected when law enforcement withdraws the request; a request is not considered rejected when a company cannot find the specified information while attempting to comply with the request.

Content Disclosed

When a company indicates that it has disclosed content in response a government request, that disclosure may also include non-content information.

Only Non-Content Disclosed

When a company indicates that it has disclosed only non-content in response to a government request, that means they have provided no content in response to the request. Anytime a company provides content information in response to a request, it should count that as "Content Disclosed" even if non-content information was also provided.

No Data Disclosed

A company can indicate that no data was disclosed when in response to a government request the company attempted to comply but could not provide data either because the account did not exist, or the data sought was not found in the account. This is different from when a request is rejected and the company did not attempt to comply with the request.