

**IN THE CIRCUIT COURT OF THE  
NINTH JUDICIAL CIRCUIT, IN AND  
FOR ORANGE, COUNTY, FLORIDA**

**ORAGANIZE NOW, INC., a Florida  
not for profit corporation, and  
STEPHANIE PORTA,**

**Case No.: 2014-CA-0100800  
Division: 33**

**Plaintiffs,**

**v.**

**TERESA JACOBS and  
ORANGE COUNTY, FLORIDA,  
A political subdivision of the State of Florida,**

**Defendants.**

---

**ORDER GRANTING DECLARATORY RELIEF**

This matter came before the Court at the November 12, 2015, expedited hearing on Plaintiffs' Emergency Complaint Seeking Declaratory Relief and the Court, having reviewed all pleadings and memoranda filed in this case, heard testimony from witnesses and argument from counsel, ORDERS and ADJUDGES as follows:

**BACKGROUND**

This case arises out of a series of public records requests made by Plaintiffs, Organize Now, Inc. and Stephanie Porta, to Orange County, pursuant to Article I, §24 of the Florida Constitution and Chapter 119, Florida Statutes. According to the Plaintiffs' Complaint, the requests were made on September 8, 2014, September 10, 2014, September 15, 2014, and September 19, 2014. The public records requests at issue were not specifically directed to Defendant, Mayor Teresa Jacobs, and she had no involvement with the responses that were made to those requests. Generally, the requests at issue related to information contained in Orange

County's "Dropbox" account, which is an electronic file sharing and storage system that allows users with the appropriate access to log in remotely to work on or review County documents that are contained within the Dropbox account.

The September 8, 2014, request asked to "inspect or obtain copies of all current and deleted items contained in the Dropbox or any other similarly-situated cloud based system that Orange County Mayor Jacobs has access to currently, or has utilized since she took her current office." The September 10, 2014, request asked for a "copy of the activity logs on the Dropbox or any other similarly-situated cloud based file sharing and/or file storage system that Orange County Mayor Jacobs has access to currently, or has utilized since she took her current office", "the 90-day deleted item log" and "a printed copy of the names of all individuals have had (sic) access or deposited any type of material into it." The September 15, 2014, request asked for "a copy of the history contained in the Events tab of any Dropbox account viewed or accessed by Mayor Teresa Jacobs or anyone working under her immediate direction and control during the time period between Jan. 4, 2011, and Sept. 13, 2014." Finally, the September 19, 2014, request asked for "(i) a list of all users for the drop box used by the Mayor's Office for the past two years; and (ii) Any audio or video files placed in drop box by Kevin Shaughnessy between July 1, 2012, and September 30, 2012, and the events timeline for the drop box used by the Mayor's office for the same time period."

While Plaintiffs' Complaint specifically references the several public records requests mentioned above, they only take issue with the County's response to the September 15, 2014, public records request as contained in the September 19, 2014, correspondence from the County Attorney's Office to plaintiff, Stephanie Porta, which reads, in pertinent part, as follows:

In response to your public records request made on September 15, 2014, enclosed you will find a CD with the requested activity log.

The IP addresses have been redacted from the log pursuant to Florida Statutes 282.318 and 501.171.

"IP" is an acronym for "Internet Protocol" and, according to expert testimony given at the hearing, an IP address is a unique code assigned to all computers, cell phones, computer tablets and certain other electronic devices which is similar to a telephone number. In this case, the redacted IP addresses would identify the specific computers or mobile devices that accessed the County's Dropbox account during the relevant time period. Plaintiffs contend that the IP addresses should not have been redacted because they are public records which do not qualify as valid exemptions from Florida's public records disclosure requirements. The County disagrees.

### LEGAL ANALYSIS

Florida has a long history of open government, dating back to the passage of its first public records law in 1909 (Chapter 5942, Acts 1909, Sec. 1). Likewise, in 1992, Article I, Section 24(a) of the state constitution was adopted which provided a constitutional guarantee to the openness of public records. Currently, Florida's public records law is codified in Chapter 119, which specifically states the intent of the legislature that "it is the policy of this state that all state, county, and municipal records are open for personal inspection and copying by any person." This policy has been applied broadly by Florida Courts in favor of public disclosure and limitations and exemptions have been narrowly construed and limited to their designated purpose. See, e.g., *Ramses, Inc. v. Demings*, 29 So. 3d 418, 421 (Fla. 5<sup>th</sup> DCA 2010).

The legislature has carved out certain exemptions from public disclosure, as contained in Chapter 119 and elsewhere, which include certain sensitive documents and information such as some collective bargaining material, medical records, certain attorney-client material, trade secrets, criminal investigation information, police complaint information and others. If in response to a public records request, the custodian of the public records claims that the records

are exempt from disclosure, the burden is on the custodian to demonstrate entitlement to an exemption from disclosure requirements. Weeks v. Golden, 764 So. 2d 633 (Fla. 1<sup>st</sup> DCA 2000). Accordingly, it is Orange County's burden here to establish an exemption from disclosure of the IP addresses at issue.

Preliminarily, in its "Trial Memorandum" the County claimed that the IP addresses do not meet the definition of "public records" set forth in §119.011(12), Florida Statutes (2014) and therefore do meet any disclosure requirement. In this regard, "public records" are defined as:

All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by an agency.

While the IP addresses may not have been "made or received pursuant to law or ordinance", it seems clear that the recording and retention of those IP addresses by the County was done as part of the work being performed by the County in its Dropbox account and, therefore, were made in "connection with the transaction of official business by an agency." There was no evidence presented to the contrary at the November 12, 2014, hearing. Accordingly, the Court finds that the IP addresses at issue are public records pursuant to Chapter 119 and the County has the burden to establish an exemption from their disclosure.

According to testimony and argument presented at the November 12, 2014, hearing and its post-hearing memorandum, Orange County seeks to establish disclosure exemption pursuant to §501.171, Florida Statutes (2014) and §119.071(1)(f), Florida Statutes (2014), individually, as well as §119.071(3), Florida Statutes (2014), and §281.301, Florida Statutes (2014), read in conjunction with each other. Each of these will be addressed separately.

**§501.171, Florida Statutes (2014)**

This statute, which went into effect this year, relates to the security of confidential personal information, and requires "covered entities" (such as Orange County) to "take reasonable measure to protect and secure data in electronic form containing personal information." The statute also requires a covered entity to provide notice to the Department of Legal Affairs of any security breach affecting 500 or more individuals in Florida.

Based on the plain language of this statute, the confidentiality provisions contained therein relied on by the County, come into play only after there has been a security breach and the County has provided the required notice of such breach to the Department of Legal Affairs. For example, the County relies on the provision of §501.171(11)(a) which provides:

All information received by the department pursuant to a notification required by this section, or received by the department pursuant to an investigation by the department or a law enforcement agency, is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution, until such time as the investigation is completed or ceases to be active. This exemption shall be construed in conformity with s. 119.071(2)(c). (emphasis added).

The County's reliance on this provision is inapplicable because the IP addresses at issue here were not received by the Department of Legal Affairs for investigation after the County had experienced a security breach. In fact, there would have been no need for the County to notify the Department of Legal Affairs in this case because there has not yet been a security breach caused by disclosure of IP addresses. While the County is justifiably concerned that disclosure of the IP addresses could lead to a security breach, the exemption contained in §501.171(11)(a) does not apply because it relates only to post breach disclosure to the Department of Legal Affairs for the purposes of investigating the security breach.

The same rationale applies to the County's reliance on §501.171(1)(c)4 which provides:

(c) Upon completion of an investigation or once an investigation ceases to be active, the following information received by the department shall remain confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution:

4. Information that would otherwise reveal weaknesses in a covered entity's data security.

Because there has been no legal affairs investigation related to the IP addresses being sought by the Plaintiffs in this case, the exemption provisions relied upon by the County in §501.171 are inapplicable.

**§119.071(1)(f), Florida Statutes (2014)**

This section relates to general exemptions from inspection or copying of public records.

The provision relied on by the County exempts certain software obtained by a state agency and exempts from public disclosure the following:

(f) Data processing software obtained by an agency under a licensing agreement that prohibits its disclosure and which software is a trade secret, as defined in s. 812.081, and agency-produced data processing software that is sensitive and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution.

In this respect, the County did not prove that the IP addresses at issue qualify as "data processing software" which is defined in §119.011(6) as "the programs and routines used to employ and control the capabilities of data processing hardware, including but not limited to, operating systems, compilers, assemblers, utilities, library routines, maintenance routines, applications, and computer networking programs." There simply was no competent evidence presented by the County that the IP addresses, by themselves, can in any way be considered exempt as "data processing software."

**§119.071(3), Florida Statutes (2014) & §281.301, Florida Statutes (2014)**

Section 119.071(3) makes confidential and exempts from public records disclosure governmental "security system plans" which are defined, in pertinent part, as:

- a. Records, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations, or consultations or portions thereof relating directly to the physical security of the facility or revealing security systems;
- b. Threat assessments conducted by any agency or private entity;
- c. Threat response plans;

Section 281.301 contains similar language as follows:

Information relating to the security systems for any property owned by or leased to the state or any of its political subdivisions ... including all records, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations, or consultations or portions thereof relating directly to or revealing such systems or information, and all meetings relating directly to or that would reveal such systems or information are confidential and exempt from ss. 119.07(1) and 286.011 and other laws and rules requiring public access or disclosure.

In support of this position, the County relies heavily on Critical Intervention Services, Inc. v. City of Clearwater, 908 So. 2d 1195 (Fla. 2<sup>nd</sup> DCA 2005) and Attorney General Opinion 04-28. In Critical Intervention Services ("CIS"), the Plaintiff filed a complaint and petition for writ of mandamus against the City of Clearwater after it was denied a portion of its public records request. After the trial court granted the city's motion to dismiss the complaint and the petition for writ of mandamus, CIS appealed. CIS, a private security company, initially made a public records request for the aggregate number of residential and business alarm permits issued by the city in 2003 and the number of warnings and citations that the city had issued for violation of the City's ordinance related to false alarms. The city complied with this request.

CIS then made a second request seeking the identity of the permit holders, as well as records showing the amounts of the fines or service charges. Although the city disclosed the total amount of fines and service charges that had been levied, it refused to disclose the identities of the permit holders. The city argued that sections 281.301 and 119.071, Florida Statutes, precluded disclosure of this information because the identity of security permit holders would allow CIS and others to identify which businesses and residences are protected by a security system and which are not, thus creating a risk to the public. Critical Intervention Services, Inc. at 1196. The city supported its position by relying heavily on Florida Attorney General Opinion 04-28.

Responding to an inquiry whether certain information, which included the names and addresses of persons or businesses cited or warned for violations of the city's alarm ordinance, and the records of police dispatches containing the addresses of locations where a verified or false alarm resulted, the Attorney General concluded, based on the express language of section 281.301, that such records were not open to either inspection or copying. In doing so, the Attorney General noted that "security plans, both public and private, are a vital part of public safety, including the safety of services, such as telecommunications, on which the public relies," and the "need to protect public and private infrastructure from terrorist attack." Likewise, "the disclosure of the names and addresses contained in the specified records would necessarily reveal the existence of security systems" (emphasis added). Op. Att'y Gen. 04-28 at 3.

In Critical Intervention Services, Inc., the Court agreed with the rationale of the Attorney General in the context of security systems and affirmed the trial court's ruling. In doing so, the Court held that sections 281.301 and 119.071 prohibit public disclosure of the names and addresses of applicants for security system permits, of persons cited for violations of alarm

ordinances, and of individuals who are the subject of law enforcement dispatch reports for verified or false alarms because disclosure would imperil the safety of persons and property. *Id.* At 1197. This holding seems logical because the public disclosure of the requested information regarding security systems would disclose to criminals which businesses and residences in Clearwater were protected by security systems and which were not, thus creating the very risk contemplated by sections 281.301 and 119.071.

The Critical Intervention Services holding is distinguishable from the present case. The information sought to be disclosed in Critical Intervention Services related directly to security systems. In fact, the Court recognized that disclosure of the information requested in that case would “necessarily reveal the existence of security systems.” Here, the County acknowledged at the hearing that IP addresses are not “security systems plans” or “security systems.” While the County has expressed a legitimate concern that disclosure of IP addresses would constitute an additional security threat because they would identify specific computers used to access Dropbox, which would then become potential targets for hacking, it also acknowledged that it already identifies 20,000 – 30,000 intrusion attempts daily and it has measures in place to deal with those attempts.

While the system that the County has in place to thwart the current onslaught of intrusion attempts would likely be exempt from public disclosure as a security system plan, that is simply not the issue before this Court. Here, the County has identified the potential for an additional security risk associated with the disclosure of IP addresses for those computers that have accessed the County’s Dropbox account. That increased risk does not create a disclosure exemption from any of the statutory authority or case law cited by the County. This is especially true in light of Florida’s policy of narrowly construing exemptions to public record disclosure. A

determination that public disclosure of IP addresses violates the statutory protection afforded to security system plans would better be addressed by the legislature through explicit statutory language rather than the judiciary.

### CONCLUSION

The IP addresses at issue here are public records and do not qualify for any exemption from disclosure set forth by Orange County. Accordingly, they should be disclosed and Plaintiffs' Emergency Complaint Seeking Declaratory Relief is hereby GRANTED. The County shall produce, within 30 days from the date of this Order, un-redacted records containing the IP addresses of the specific computers or devices that accessed the County's Dropbox account during the relevant time period. The Court reserves ruling on the award of attorneys' fees and costs to be addressed at a future hearing if either party so requests.

ORDERED and ADJUDGED in chambers this 23<sup>rd</sup> day of November, 2014.

  
\_\_\_\_\_  
Robert J. Egan, Circuit Judge

Conformed copies to:

Andrea Flynn Mogensen  
200 S. Washington Blvd., Suite 7  
Sarasota, FL 34236

William C. Turner, Jr.  
Assistant County Attorney  
201 S. Rosalind Avenue, 3<sup>rd</sup> Floor  
Orlando, FL 32801

Edward A. Dion  
110 East Broward Blvd., Suite 1700  
Ft. Lauderdale, FL 33301