THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 9 | Number 2 Article 16

2014

Evidentiary Power and Propriety of Digital Identifiers and the Impact on Privacy Rights in the United States

Michael Losavio
University of Louisville

Deborah Keeling
University of Louisville

Recommended Citation
Losavio, Michael and Keeling, Deborah (2014) "Evidentiary Power and Propriety of Digital Identifiers and the Impact on Privacy Rights in the United States," *Journal of Digital Forensics, Security and Law*: Vol. 9 : No. 2 , Article 16.
DOI: https://doi.org/10.15394/jdfsl.2014.1181
Available at: https://commons.erau.edu/jdfsl/vol9/iss2/16

EVIDENTIARY POWER AND PROPRIETY OF DIGITAL IDENTIFIERS AND THE IMPACT ON PRIVACY RIGHTS IN THE UNITED STATES

Michael Losavio and Deborah Keeling
University of Louisville
Department of Justice Administration
Louisville, KY 40204, USA
{michael.losavio, deborah.keeling}@louisville.edu

ABSTRACT

Media and network systems capture and store data about electronic activity in new, sometimes unprecedented ways; computational systems make for new means of analysis and knowledge development. These new forms offer new, powerful tactical tools for investigations of electronic malfeasance under traditional legal regulation of state power, particular that of Fourth Amendment limitations on police searches and seizures under the U.S. Constitution. But autonomy, identity and authenticity concerns with electronic data raise issues of public policy, privacy and proper police oversight of civil society. We examine those issues and their implications for digital and computational forensics

Keywords: identity, authentication, digital, computation, forensics, probable cause, privacy, security, search, seizure

1. INTRODUCTION

Privacy is "the right to be left alone" (Brandeis and Warren, 1890). Fundamental to that right are restrictions on state power to intrude into personal affairs. The hallmark is the Fourth Amendment and its limitations on domestic police searches and seizures under the U.S. Constitution set forth at the founding of the Republic more than two hundred years ago. Prophetically, Justice Brandeis in 1928 warned of progress in science that would lead to unimagined invasions of personal privacy (Olmstead v. United States, 277).

Restrictions on intrusions into the "private" activities of people do not necessarily apply to non-content related material disclosed to third parties or data transfers across borders nor are they limited to those set out in the federal constitution. National security needs may impact access to activities otherwise protected by the Fourth Amendment. Statutory protections, federal and state, may exceed or refine Fourth Amendment protections, such as under the Electronic Communications Privacy Act and the Foreign Intelligence Surveillance Act.

The hallmark is that the Fourth Amendment prohibits *unreasonable* searches and seizures. What is reasonable or unreasonable may not be easily or algorithmically defined for the vast, diverse scope of human actions. It generally permits a thorough police search of a person's home, person, papers and effects only where there is probable cause that evidence of a crime may be found or that person has committed a crime. Lesser kinds of intrusions may be justified by the lesser standard of objective facts supporting reasonable suspicion. And the use of data for inferences need meet no standard as to make someone a "person of interest" in an investigation.

The growth of massive data sets and powerful analytics has led to practical changes in the profiling of individuals in ways never anticipated. Ohm notes as to access to personal information on one's life, "Today's technology poses a constitutional puzzle that is different in kind, not just in

degree, from the one solved only a few decades ago" (Ohm, 2011). Given the massive data storage and analytic capabilities of systems, traditional police investigative conduct and search warrants, with their traditional particularity requirements, are morphing into what some consider the functional equivalent of intrusive general warrants of search so hated by the Founders of the Republic.

If a person's data life is engaged in a cloud system, then search of that system can be a search, analysis and conclusion on an entire personal life.

Similarly, personal electronic devices, most commonly a cellular telephone, can hold massive amounts of information about one's personal life in ways never before anticipated. Connected to other systems, they are the data life of their holders. Conversely, some argue that vetted computational systems can bring greater accuracy and less bias to forensic analysis as it extends investigative powers (Srihari, 2010). It can even serve to support the "digital innocence" of a subject wrongfully accused (Fairfield and Luna, 2014).

The digital age uses digital *facts*, particularly items such as addressing numbers under the Internet Protocol, GPS location data and alphanumerical identifiers used for authentication and identification in online transactions. These artifacts become the evidence used for making such determinations to search or seize. Given the technical issues with evidence preservation and examination in electronic storage media, search warrants relating to computing systems may direct the seizure of computers and data collections and removal off-site for examination in a computer forensics facility.

These digital facts include the metadata and transactional data associated with electronic activity. These may be independent of any content of the electronic transaction but still sufficient, in direct or circumstantial context,

The combination of these circumstances has led to the search of homes and businesses and seizure the computers therein based on finding a credit card number, e-mail address or IP address in system data of contraband servers. Little other indicia of the identity or authentication of the transaction is needed for the issuance of a warrant for search and seizure.

This reliance on simple digital identification with minimal authentication further corrodes privacy and liberty rights in new ways.

2. "PROBABLE CAUSE" THAT A COMPUTER CRIME HAS BEEN COMMITTED AND A STATE INVASION OF A PERSON'S HOME, PERSON AND COMPUTERS IS JUSTIFIED

Electronic evidence alone or matched with other evidence may indicate a crime and additional evidence of that crime. That additional evidence, once obtained, can correlate the electronic record with other actions. This correlation and development role is particularly important for remote data collected over networks; correlation to other evidence is a key function of electronic evidence in prosecuting a digital crime (Carrier, 2005). Absent special circumstances, the search or seizure of a person or his effects without consent is illegal in the U.S. unless

1) an application under oath is made
2) before a neutral magistrate that
3) details facts that establish "probable cause" to believe a crime has been committed and evidence of that crime will be found in the place searched and things seized.

"Probable cause" itself means a "fair probability" under a common sense analysis that evidence is to be found at the place to be searched; this was defined as being less that the "preponderance of the evidence" standard to support other judicial findings (Illinois v. Gates, 462). An application for a search is to be judged under the "totality of the circumstances" presented. *Id.*

With the accumulation of network forensic and system data in so many forms, as well as the volatility and multiplicity of that data, what data is sufficient to say there is a fair probability that a particular network or system user has contraband or evidence of a crime on his or her computer? Once that quantum is defined, police power is essentially unlimited once that measure is met by evidence.

This sensitivity to constitutional principles is most strenuously tested when looking at the "heroin of cyberspace," child pornography (Howell, 2004). It is one of the most inflammatory misuses of networks; it is useful for analysis precisely because it is a crime to have it in digital possession (Losavio, 2005).

2.1 The Boundaries of "Fair Probability" of Digital Evidence of Crime

A series of court cases in the United States have approved the powerful tactical use of electronic data to justify issuance of warrants to search and seize computers. These cases push the boundaries of the Fourth Amendment and notions of identity and authentication in digital environments. They rely on system-collected data independent of actual network transactions of downloading or uploading contraband.

These tools raise issues of law, public policy and privacy as to proper police oversight of civil society. There is concern generally that existing rules fail to properly deal with digital evidence (Kerr, 2005). ""In the old days, the laws against illegal search and seizure were interpreted much more strictly," one defense counsel notes, "but as this technology develops, the definition of probable cause will most likely be expanded"" (Silberman, 2002).

The boundaries of "Fair Probability" of the existence of criminal evidence are strained by decisions of the U.S. Courts. The U.S. Court of Appeals for the Ninth Circuit held, in essence, that on-line membership information describing a particular person in a child pornography website was sufficient to justify the search and seizure of that person's computer. (United States v. Gourde, 440). The Court of Appeals for the Second Circuit said "It is common sense that an individual who joins such a site would more than likely download and possess such material" (United States v. Martin, 426).

But the Ninth Circuit's case, *United States v. Gourde*, had no evidence of network activity transferring contraband files to Gourde's computer, either through express download/ftp transfer, e-mail or simple http transfer via the web browser.

This case provoked both dissent and public concern over the boundaries of network-transmitted data and user liability (Maclean, 2006).

2.2 General Principle or Fact Specific – The Affidavit for the Search

Gourde pled guilty to possession of 100 computer images of child pornography, violations of 18 U.S.C. §§ 2252 and 2252A, but reserved the right to challenge the FBI's seizure of his computer, where the definitive evidence of his crime was found. If Gourde showed there was no probable cause to believe there was evidence of a crime on his computer, the seizure and search would have been illegal and the evidence found could not be used against him; as there was no other evidence, his conviction would not stand and he would be released.

What distinguished Gourde's case from others was that there was no direct evidence of possession of these illegal images by Gourde. Gourde's "steps to affirmatively join" the website, were shown by membership data, which included his credit card, via a web page showing questionable material.

What was not raised in the affidavit was any evidence that Gourde had actually downloaded child pornography images or that it was Gourde himself that had joined the website.

Similarly, in the Second Circuit's case *United States v. Martin*, the supporting affidavit was deemed sufficient where it showed there was evidence "that an e-mail

address of a "girls12-16" member was linked to Martin's house..."

Thus identification data with minimal authentication may support the issuance of a state warrant to search and seize an implicated computer system. Yet the Court of Appeals did note that

> The internet is not a safe haven for illicit conduct. Rather, it is a digital community where the zeros and ones that translate into visible and audible expressions have legal consequences. Although we will be diligent to guard against unlawful searches and seizures, even at the digital divide, the internet does not present an exception to established principles of probable cause. *Id.*, at 89

This remains the standard relating to issuance of search warrants relating to activity associated with digital contraband and IP address identification (United States v. Robinson, United States v. Strausbaugh, & United States v. Valley). Indeed, combined with the persistence of electronic evidence in certain media, the traditional doctrine of "staleness," that old information is unreliable as to establish a fair probability that evidence might still be in a particular location, applies differently to electronic and digital evidence; old information too stale to support a warrant for physical evidence will still support a warrant for digital artifacts that may be cast about and persist in their related media (United States v. Valley).

2.3 FISA Warrants

Similar concerns relate to domestic surveillance under orders issues by the Foreign Intelligence Surveillance Act (FISA) and the FISA court. Transactional metadata for international communications fall outside of Fourth Amendment and statutory protections under U.S. law, but if those lead to purely domestic communications where metadata and content data are needed then a court ordered is needed. The issue is determining the quantum of evidence, particularly inferences from metadata, that support issuance of such orders. A related issue is the what should be done with data producing non-criminal inferences that still may impact the privacy of one's affairs and what, if any, limits should be placed on that by statute or common law construction.

3. IMPLICATIONS FOR PRIVACY AND SECURITY

These cases imply an exceptionally low standard of electronic evidence in support of the power of the search warrant. The ease of fabrication of electronic evidence goes far beyond what is possible with other media and is accomplished through common, non-technical means (Losavio, 2006). This creates a possibility for exceptional abuse through the application of police power. Cyber extortion using child pornography is a global issue (The Straits Times, 2005; The Toronto Star, 2003; Wright, 2005). Such standards offer opportunities to abuse through planted and spoofed evidence without incentive to authenticate data or correlate it to other evidence of criminal activity.

On the other hand, the shear poison of child pornography may lead the courts and justice agencies to treat it differently than other criminal activity such that this seemingly lesser standard does not apply elsewhere. Yet when this material falsity was raised in *Martin*, and other cases, the courts relied on system data to validate police action.

Judge Poole's dissent in *Martin* accuses the court of creating just such an exception; the danger is that this exception might become the rule.

Reliance on such minimally authenticated digital data has contributed to the expansion of "identity theft," itself both a financial crime and a violation of personal privacy through the false exploitation of another's good name, credit history and right not to be hassled by bill collectors. Now it may justify expansion of state invasions of personal privacy.

Caloyannides notes with digital evidence "The potential for a miscarriage of justice is vast," (Caloyannides, 2004). As the U.S. Supreme Court observed in a denying immunity to government agents for the

seizure of computers and their subsequent destruction during examination:

> Susan Hallock owned a computer software business that she and her husband, Richard, operated from home. After information about Richard Hallock's credit card was stolen and used to pay the subscription fee for a child pornography Web site, agents of the United States Customs Service, investigating the Web site, traced he payment to Richard Hallock's card and got a warrant to search the Hallocks' residence. With that authority, they seized the Hallocks' computer equipment, software, and disk drives. No criminal charges were ever brought, but the Government's actions produced a different disaster. When the computer equipment was returned, several of the disk drives were damaged, all of the stored data (including trade secrets and account files) were lost, and the Hallocks were forced out of business (Will v. Hallock, 2006).

But that miscarriage of justice can be far worse, with conviction and imprisonment based on digital contraband on a computer a person may not have had dominion over. An appalling example is the *Amero* case, where a substitute seventh-grade teacher was convicted of four felonies of exposing minors to pornography on the classroom computer based on erroneous testimony that pornography pop-ups can only be fetched by intentionally and deliberately accessing the material (Krebs, 2014). After facing up to 40 years in prison, Ms. Amero was granted a new trial based on testimony and analysis by computer specialists that refuted that claim and found both lapsed firewall, anti-virus and spyware protection on the computer and various spyware programs; her attorney observed

> The lesson from this is: All of us are subject to the whims of these computers, these great machines that all of a sudden can create a criminal case against someone like Julie, who didn't understand what was going on (Fox News, 2007).

Some of these concerns were presaged in the GPS tracking and analytics case of *United States v. Jones,* where several justices commented on the change in privacy relations that may be created by computational. The Supreme Court in *United States v. Jones* required a search warrant to justify the placement of an electronic tracking device on a suspect's vehicle, holding it constituted a physical trespass permitted only upon finding of probable cause. But in that opinion Justice Sonja Sotomayor further suggested the need to reconsider what privacy means in an era of massive third party data collection and analysis. (concurring opinion, *United States v Jones*). Jones dealt with one facet of the new data reality, that of the massive and inexpensive collection of positional GPS data and analytics to quickly produce a profile of a subject's activities. Equally applicable to the growing data and analytical power of digital forensics, Justice Sotomayor wrote:

> The net result is that ...—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society."

The Supreme Court directly addressed these concerns as to the requirements to search massive portable data collections in mobile cellular telephones in the 2014 cases of *Riley v. California* and *United States v. Wurie*, where it held illegal the warrantless search of a cellular telephone seized from an arrestee, distinguishing a cell phone search from a traditional search incident to an arrest.

The touchstone of the analysis by the Supreme Court was this balancing of interests "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental

interests."(citing *Wyoming* v. *Houghton*, 526 U. S. 295, 300 (1999)). In declining to apply prior precedent that upheld a search of items found on a person incident to their arrest, the Supreme Court found that cell phone technology, including its uniquely personal and massive data profile, did not present any risk of the destruction of evidence or danger to an officer that outweighed the privacy interests of the phone's owner that were enlarged from other personal artifacts by the nature of the vast data storage. Thus a search of a cell phone by police is unreasonable absent a warrant based upon probable cause that the cell phone held evidence of a crime or was itself an instrumentality of a crime.

Similarly, the limits, if any, to electronic surveillance by the National Security Agency, may be subject to Supreme Court analysis. These will further define digital and computational forensic practice and the privacy of people within this domain.

4. CONCLUSION

We now live in a new space of information density, one where relatively inexpensive technologies can give every government the surveillance powers possessed by the old German Democratic Republic's Stasi and the current regime of North Korea. This may have an impact on how people relate to each other and to how we are governed.

In the United States, the Fourth Amendment to the Constitution of the United States limits the power of police to search and seize a person, his computer and related transaction/content data:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. IV Amend. (1791)

Technical security cannot protect privacy and security with such attitudes towards data. Security policy must extend into all domains of society. The challenge will be to establish a balance where courts set a stricter boundary for state searches and seizures based on electronic evidence of questionable reliability.

The *Gourde* court observed

> ... Given the current environment of increasing government surveillance and the long memories of computers, we must not let the nature of the alleged crime, child pornography, skew our analysis or make us "lax" in our duty to guard the privacy protected by the Fourth Amendment. We are acutely aware that the digital universe poses particular challenges with respect to the Fourth Amendment.

The Supreme Court in *United States v. Jones* and *Riley v. California* established bounds for those challenges, albeit within the traditions of our Constitution. That awareness still needs greater knowledge of the facts of identity and authenticity of electronic data as evidence, its mutability and evanescence, if the rights and liberties and privacy of citizens are to be honored. That may be further developed with rulings on the limits that may be placed on FISA surveillance of the lives of the many (Hurley, 2014).

The future regulation of the informational lives of everyone will shape how the relationships between citizen and government evolve.

REFERENCES

Brandeis, L., & Warren, S. (1890). The Right to privacy, IV. *Harvard Law Review*, *5*.

Caloyannides, M. (2004). *Privacy Protection and Computer Forensics*. 2nd ed. Artech House.

Carrier, B. (2005). *File System Forensic Analysis*. Addison Wesley.

Fairfield, J., & Luna, E. (2014). *Digital Innocence*. 99 Cornell L. Rev 981 (July 2014).

Fox News. (2007). Connecticut teacher gets new trial on web-porn charges. Retrieved on August 22, 2014 from

http://www.Foxnews.Com/Story/0,2933, 278897,00.Html

Howell, B. (2004). Real world problems of virtual crime. *9 Int'l J. Comm. L. & Policy*, *5*.

Hurley, L. (2014). Two U.S. justices say high court will likely rule on NSA programs. Reuters News Service, April 17, 2014.

Illinois v. Gates, 462 U.S. 213, 230, 246 (1983).

Kerr, O. (2005). Digital evidence and the new criminal procedure. 1*05 Colum. L. Rev.*, 279.

Krebs, B. (2014). Substitute teacher faces jail time over spyware, Retrieved on August 22, 2014 from http://blog.washingtonpost.com/securityfix/2007/01/substitute_teacher_faces_jail.html

Losavio, M. (2006). Non-technical manipulation of digital data - Legal, ethical and social issues. IFIP International Conference of Digital Forensics 2005, 51-63. *Advances in Digital Forensics*, Springer 2006.

Losavio, M. (2005). The law of possession of digital objects: Dominion and control issues for digital forensics investigations and prosecutions. First International Workshop on Systematic Approaches to Digital Forensic Engineering, 177-183. Retrieved from http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=33521& isYear=2005

Maclean, P. (2006). Strong dissent in computer search case; Warrant based only on Web site membership. *National Law Journal*, April 3, 2006, NEWS, 6.

Ohm, P. (2011). Massive hard drives, general warrants and the power of magistrate judges. *97 Va. L. Rev.* In Brief 1, 8 (2011).

Olmstead v. United States, 277 U.S. 438, 473-475 (1928) (Justice Brandeis, dissenting)

Riley v. California, (2014) ____ U.S. ____

Silberman, S. (2002). The United States of America v. Adam Vaughn Wired Magazine, Issue 10.10, Oct 2002.

Srihari, S. (2010). Beyond C.S.I.: The rise of computational forensics pattern recognition and other computational methods can reduce the bias inherent in traditional criminal forensics. IEEE Spectrum, December, 2010.

The Straits Times. (2005). Racketeers and gangs prowling cyberspace. Singapore. February 23, 2005.

The Toronto Star. (2003). Wave of Cyberblackmail Hitting Offices. December 30, 2003.

United States v. Gourde, 440 F.3d 1065 (9th Cir. 2006)

United States v. Jones, (2012). 565 U.S. ___

United States v. Martin, 426 F.3d 68, 75, reh. Denied 426 F.3d. 83 (2d Cir. 2005)

United States v. Robinson, 741 F.3d 588 (5th Cir. 2014)

United States v. Strausbaugh. (2013). U.S. App. LEXIS 16553 (unpublished 3rd Cir. 2013)

United States v. Valley, 755 F. 3d 581 (7th Cir. 2014).

Will v. Hallock. (2006). 546 U.S. 345

Wright, C. (2005). An online scam that can ruin your life. Retrieved on June 2005 from http://www.marketingsource.com/articles/view/1259

