

COMMONWEALTH OF MASSACHUSETTS
SUPREME JUDICIAL COURT
NO. SJC-11358

COMMONWEALTH
Appellee

v.

LEON GELFGATT Defendant-
Appellant

ON REPORT OF A QUESTION OF LAW BY THE SUPERIOR COURT
FOR SUFFOLK COUNTY PURSUANT TO MASS. R. CRIM. P. 34

BRIEF *AMICUS CURIAE* FILED BY DANIEL K. GELB, ESQUIRE AND
DANIEL B. GARRIE, ESQUIRE TO WHICH NATIONAL ASSOCIATION
OF CRIMINAL DEFENSE LAWYERS JOINS IN SUPPORT OF
DEFENDANT-APPELLANT

Daniel K. Gelb
(BBO# 659703)
GELB & GELB LLP
84 State Street
Boston, MA 02109
(617) 345-0010 (T)
(617) 345-0009 (F)
dgelb@gelbgelb.com

Daniel B. Garrie, Esq.
LAW & FORENSICS
Senior Managing Partner
6506 3rd Ave NW, Suite C
Seattle, WA 98117
(215) 280-7033 (T)
daniel@lawandforensics.com

August 23, 2013

TABLE OF CONTENTS

TABLE OF CONTENTS _____ ii

TABLE OF AUTHORITIES _____ iii-iv

INTEREST OF THE *AMICI CURIAE* _____ 5

ISSUE PRESENTED _____ 5

SUMMARY OF THE ARGUMENT _____ 6

ARGUMENT _____ 8

 I. Computer Technology Underlying Modern Electronic Password Encryption

 A. Definition Of A "Computer" And How One Works

 B. Evolution Of Electronic Password Encryption Technology And Unique Characteristics Of Protected Data

 C. The "Point Of Encryption" And How It Is Accomplished By The User

 II. Compelling A Password Production To The Commonwealth Is A Violation Of Defendant's Right Against Self-Incrimination Pursuant To The Fifth Amendment Of The United States Constitution And Article 12 Of The Massachusetts Declaration Of Rights

 III. Society Has Adopted An Objective Expectation Of Privacy In Computer Passwords And Encrypted Data Protected By The Fourth Amendment Of The United States Constitution And Article 14 Of The Massachusetts Declaration Of Rights

CONCLUSION _____ 22

APPENDIX A _____ 23

APPENDIX B _____ 26

MASS. R. A. P. 16(k) CERTIFICATION _____ 28

CERTIFICATE OF SERVICE _____ 29

TABLE OF AUTHORITIES

Cases

<i>Advent Systems Ltd. v. Unisys Corp.</i> , 925 F.2d 670 (3rd Cir. 1991)	8
<i>Apple Computer, Inc. v. Franklin Computer Corp.</i> , 714 F.2d 1240 (3d Cir. 1983)	9
<i>Bell v. Wolfish</i> , 441 U.S. 520 (1979)	16
<i>Bernstein v. U.S. Dept. of State</i> , 922 F. Supp. 1426 (N.D. CA 1996)	12
<i>Commonwealth v. Bertini</i> , 466 Mass. 131 (2013)	15
<i>Commonwealth v. Maxwell</i> , 441 Mass. 773 (2004)	15
<i>Fantasy Sports Props., Inc. v. SportsLine.com, Inc.</i> , 287 F.3d 1118, (Fed. Cir. 2002)	8, 9
<i>Fisher v. United States</i> , 425 U.S. 391 (1976)	16, 21
<i>In re Aimster Copyright Litigation</i> , 334 F. 3d 643 (7th Cir. 2003)	13
<i>Junger v. Daley</i> , 209 f. 3d 481 (6th Cir. 2000)	11
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	20, 21
<i>Lotus Dev. Corp. v. Paperback Software Int'l</i> , 740 F. Supp. 37 (D. Mass. 1990)	9
<i>Maryland v. King</i> , 133 S. Ct. 1958 (2013)	15, 20
<i>Massiah v. United States</i> , 377 U.S. 201 (1964)	16
<i>Microsoft Corp. v. AT&T Corp.</i> , 550 U.S. 347(2007)	8
<i>Ricoh Co., Ltd. v. Quanta Computer Inc.</i> , 550 F.3d 1325 (Fed. Cir. 2008)	8
<i>Schneckloth v. Bustamonte</i> , 412 U.S. 218 (1973)	17
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979)	21
<i>Trulock v. Freeh</i> , 275 F.3d 391, 403 (4th Cir. 2001)	13
<i>U.S. v. Carson</i> , No. 12-cr-30089 (C.D. Ill. Oct. 25, 2012)	8
<i>United States v. Buckner</i> , 407 F. Supp. 2d 777 (W.D. Va. 2006)	17
Massachusetts Statute	
M.G.L. c. 266 § 120F	18, 19

Other Authorities

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (U.S. Dept. of Justice) (2009 ed.) _____ 15

Federal Information Processing Standards Publication 197, Advanced Encryption Standard (Nov 26, 2001) _____ 12

Treatises

David Salomon, *Data Privacy and Security: Encryption and Information Hiding*, (Springer, May 20, 2003) 4, 133 _____ 11, 12

Randall Davis, *The Nature of Software and Its Consequences for Establishing and Evaluating Similarity*, 5 *Software L.J.* 299, 302 (Volume V Issue 2, April 1992) _____ 9

James H. Ellis, *The history of non-secret encryption*, 23 *Cryptologia* 267 (1999) _____ 11

Michael Hart, Pratyusa Manadhata and Rob Johnson, *Text classification for data loss prevention*, PETS'11 Proceedings of the 11th international conference on Privacy enhancing technologies (2011) _____ 13

Jonathan Katz, Yehuda Lindell, *Introduction to Modern Cryptography* 5 (2008) _____ 12, 13

Patterson and Hennessy, *Computer Organization and Design: The Hardware/Software Interface*, at p. 24 (4th ed. 2009) _____ 8

Reinhard Wobst, *Cryptology Unlocked* 19 (2001) _____ 11

U.S. Dept. of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009 ed.) _____ 14

Constitutional Provisions

Article XII of the Massachusetts Declaration of Rights _____ 6, 13, 14, 18

Article XIV of the Massachusetts Declaration of Rights _____ 7, 19

Fifth Amendment to the United State Constitution _____ 5, 6, 13, 14, 15, 17, 18

Fourth Amendment to the United States Constitution _____ 6, 14, 15, 18, 19, 21

Sixth Amendment to the United States Constitution _____ 16

INTEREST OF THE AMICI CURIAE

Amici Daniel K. Gelb, Esquire; Daniel B. Garrie, Esquire; and National Association of Criminal Defense Lawyers have a particular interest in the constitutional issues relating to representation of individuals and businesses coping with the manner present day computer and mobile technologies are recalibrating the application and scope of an individual's constitutional rights against self-incrimination and unlawful encroachment by law enforcement. *Amici* respectfully submit that compelling a defendant to decrypt a password-protected piece of computer hardware, either physically by oneself, or by providing the password to the Commonwealth, would compromise one's right against self-incrimination and to be free from an unlawful search and seizure. Therefore, *Amici* respectfully urge this Honorable Court to adopt the principle in the instant case.

ISSUE PRESENTED

Whether compelling a criminal defendant to provide a password for a piece of encrypted computer hardware seized by the Commonwealth violates one's right against self-incrimination provided by the Fifth Amendment to the United States Constitution and Article Twelve of the Massachusetts Declaration of Rights?

SUMMARY OF THE ARGUMENT

Without the Commonwealth first making a showing that it has independent knowledge of both the nature of electronically stored information ("ESI") it seeks to seize and the exact location where the ESI resides on a computer's hard drive, compelling the Defendant to furnish a password to an encrypted computer, which is otherwise inaccessible by another party, violates a defendant's rights against self-incrimination and unlawful search and seizure pursuant to the Fifth and Fourth Amendments to the United States Constitution, as well as a defendant's rights under Articles 12 and 14 of the Massachusetts Declaration of Rights.¹

Compelling a criminal defendant to be the sole source of his own incrimination—particularly in the context of litigation—would be *per se* testimonial in violation of a defendant's Fifth Amendment protection against self-incrimination. Moreover, there is no less restrictive means to avoid or mitigate the violation of such a bedrock constitutional right which right every individual in the United States enjoys. The issue presented in this case is different than cases concerning the collection of DNA samples. In the DNA cases the Commonwealth

¹Text of constitutional provisions and Massachusetts statutory content addressed herein are contained in APPENDIX B attached hereto.

seeks confirmation of the source of a questioned specimen or piece of evidence. In this case, however, the issue is the compulsion of self-incriminating evidence in contradiction of well-settled constitutional doctrine such as the "act of production" privilege.

Lastly, if the Commonwealth is unable to offer proof as to the nature and content of ESI sought (e.g., specific file types, the location where the data resides in the computer's directory, etc.), the Court would endorse the Commonwealth's ability to engage in a fishing expedition on computer hardware which may contain statutorily protected ESI, such as attorney work-product and client communications.

Without knowing the nature and location of ESI on a computer, the Commonwealth should not be allowed to seek the compulsion of access to a defendant's computers given the particular use of a computer (e.g., for business) and the likelihood that the ESI residing on it is categorized as "private" by statute (e.g., attorney-client files, medical records, financial data, etc.). For the reasons set forth herein, Amici respectfully request that the issue presented be answered in the **NEGATIVE**.

ARGUMENT

I. Computer Technology Underlying Modern Electronic Password Encryption

A. Definition Of A "Computer" And How One Works.

A computer is divided into hardware and software. Computer hardware is any processing machine that accepts and translates input symbols and executes an action.² The inputs are processed according to a sequence of instructions called software.³ In a computer, hardware includes all of the equipment that comprises the physical body of the computer, its electronic circuitry and peripheral items, such as keyboards, readers, scanners, and printers.⁴ Such hardware is of limited value without software. It is the software that produces a given result, such as outputting symbols, or performing an action.⁵ The input and output symbols can represent, among other things, numbers, characters in a text

² See Patterson and Hennessy, *Computer Organization and Design: The Hardware/Software Interface*, at p. 24 (4th ed. 2009); Davis, *The Nature of Software and Its Consequences for Establishing and Evaluating Similarity*, 5 *Software L.J.* 299, 302 (1992);

³ See *Ricoh Co., Ltd. v. Quanta Computer Inc.*, 550 F.3d 1325, 1335 (Fed. Cir. 2008) (citing *Microsoft Corp. v. AT&T Corp.*, 550 U.S. 347, 127 S.Ct. 1746, 1754, 167 L.Ed.2d 737 (2007)).

⁴ See *U.S. v. Carson*, No. 12-cr-30089 (C.D. Ill. Oct. 25, 2012); *Advent Systems Ltd. v. Unisys Corp.*, 925 F.2d 670, 674 (3rd Cir. 1991).

⁵ See *Microsoft Corp. v. AT&T Corp.*, 550 U.S. 347, 127 S.Ct. 1746, 1754, 167 L.Ed.2d 737 (2007) (defining software); *Fantasy*

message, pictures in an email, the music played when your mobile phone rings, or the GPS coordinates in your car.

Computer hardware can seem endlessly complex to the uninitiated. Today, computing technology is evolving at blistering speeds from the introduction of DNA computers to Google Glass™.⁶

Software is written in several levels of complexity, with the simplest level being binary code. Binary code is the lowest level programming language that hardware understands and is written using only 1s and 0s.⁷ More complex code is written on top of binary code and allows software developers and programmers to create increasingly complex applications. Among these applications is the ability to encrypt data, whether it is stored on a hard drive or sent via email.

Sports Props., Inc. v. SportsLine.com, Inc., 287 F.3d 1118, (Fed. Cir. 2002)

⁶ This evolution was somewhat predicted in the famous "Moore's law", which states that over the history of computing hardware, the number of transistors on integrated circuits doubles approximately every two years.

⁷ The "lowest" level computer programming language is machine language, which is a binary language written in "bits". See *Lotus Dev. Corp. v. Paperback Software Int'l*, 740 F. Supp. 37, 43 (D. Mass. 1990). The third, or lowest level computer language, is machine language, a binary language using two symbols, 0 and 1, to indicate an open or closed switch (e.g., "01101001" means, to the Apple, add two numbers and save the result). *Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240, 1243 (3d Cir. 1983). Programming languages ability to deliver a result rest in part on how the programming language defines terms. See generally, Garrie, S. A. (2012). *U.S. Patent Application 13/418,541*.

B. Evolution Of Electronic Password Encryption Technology And Unique Characteristics Of Protected Data.

Encryption technology has multiple purposes, chief among them being protecting and authenticating information. A familiar form of electronic authentication is the use of passwords to restrict access to an individual computer or a network of computers. Passwords have been used for authentication well before the existence of computers. For example, sentries used to require a password to gain entrance to a particular area. Often failure to get password right had drastic consequences.

Encryption offers a mechanism for the transmission of data in an encrypted or secure manner.

C. The "Point Of Encryption" And How It Is Accomplished By The User.

Securing data in modern times has taken on a number of implementations. From physical security of isolating computers with limited keycard access and a security guard, to password protection on mobile phones, to encryption of hard drives and email communications, the means and methods to secure data are constantly advancing to offer improved security.

Encryption serves as a barrier to prevent unauthorized access to the underlying information. Historically, varying degrees of encryption have been used since (at least) ancient

times. Caesar used an eponymous cipher⁸ to send messages during battle.⁹ This cipher used a rule where the sender replaced each letter with another letter in the alphabet. The receiver simply had to reverse this process to decode the message.¹⁰ For example, in a +4 schema, each letter in the message would be replaced by letters four places down in the alphabet. The message "Hello" would then be encoded as "LIPPS".

Since Caesar's time, many forms of encryption have come and gone. Modern day encryption ciphers, or algorithms, are complex instructions that often translate the encoded text through multiple repetitions of encoding.¹¹ This is done through the combined use of an algorithm and one or more keys.¹²

⁸ David Salomon, Data Privacy and Security: Encryption and Information Hiding 4 (2003) (defining cipher simply as a "rule that tells how to encode each letter in a message.").

⁹ James H. Ellis, The history of non-secret encryption, 23 *Cryptologia* 267 (1999).

¹⁰ Reinhard Wobst, Cryptology Unlocked 19 (2001).

¹¹ Junger v. Daley, 209 f. 3d 481 (6th Cir. 2000) (stating, "Most encryption today uses an algorithm, a mathematical transformation from plaintext to ciphertext, and a key that acts as a password.")

¹² The modern standard algorithm used is the Advanced Encryption Standard (AES). For a thorough description of how this algorithm operates, see Federal Information Processing Standards Publication 197, Advanced Encryption Standard (Nov 26, 2001), available at, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

A private or secret key is input into the algorithm to make the encryption unique to that data set.¹³ Much like a password, the key must be kept secret in order to maintain the integrity of the encrypted information. However, unlike a password that a user creates, a single 128-bit key contains 16 two-character sets, that might look like this: 2b 7e 13 28 re 2i 45 q0 ab f7 15 88 09 cf 4f 3c.¹⁴

The number of keys (one or two) determines whether the encryption is symmetric or asymmetric. Symmetric encryption uses the same key to encode and decode the data.¹⁵ Asymmetric encryption involves separate keys to encode and decode the

¹³ Much like Caesar's algorithm of letter shifting, knowing that the algorithm calls for the recipient to shift letters isn't enough, in essence the key is the number of letters that must be shifted. This is known as Kerckhoff's Principle. For further reading on this principle, see Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography 7 (2008).

¹⁴ For a visual example of the encryption and decryption process using AES, see the Federal Information Processing Standards Publication 197, Advanced Encryption Standard, Appendix A-C (Nov 26, 2001), available at, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

¹⁵ David Salomon, Data Privacy and Security: Encryption and Information Hiding 133 (2003) (defining symmetric encryption as "us[ing] the same key for encryption and decryption"). See also, Bernstein v. US Dept. of State, 922 F. Supp. 1426 (N.D. CA 1996) (denying a motion to dismiss where plaintiff brought action seeking relief from a prohibition to distribute symmetric encryption software outside the US).

data.¹⁶ Either symmetric or asymmetric encryption can be used regardless of whether the data is *in motion*¹⁷ (emails, attachments to emails, etc) and *at rest*¹⁸ (files stored on a hard drive).¹⁹

II. Compelling A Password Production To The Commonwealth Is A Violation Of Defendant's Right Against Self-Incrimination Pursuant To The Fifth Amendment Of The United States Constitution And Article 12 Of The Massachusetts Declaration Of Rights.

Unlike ESI in and of itself, a computer password—if properly maintained and kept private—does not become accessible *per se* through third-party consent. Unlike ESI actually residing on the computer, a password itself—once established—is only known and maintained by the user of the operating system residing on the computer. For example, in *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001) the United States Court of Appeals for the

¹⁶ Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography 5 (2008) (defining asymmetric encryption “where the sender and receiver do not share any secrets and different keys are used for encryption and decryption”).

¹⁷ Michael Hart, Pratyusa Manadhata, and Rob Johnson. Text classification for data loss prevention, Privacy Enhancing Technologies 4 (2011) (defining data in motion as “enterprise data contained in outbound network traffic such as emails, instant messages, and web traffic.”), available at: <https://www.hpl.hp.com/techreports/2011/HPL-2011-114.pdf>

¹⁸ Hart at 4 (defining data at rest as “static data stored on [...] devices”).

¹⁹ *In re Aimster Copyright Litigation*, 334 F. 3d 643 (7th Cir. 2003) (discussing encryption software for email communications).

Fourth Circuit held that password-protected computer files are analogous to "locked footlockers" inside a bedroom. Typically, such ESI would be considered outside the scope of consent through a third party with "common access." However, specific facts may overcome an individual's expectation of privacy even in password-protected files if the computer hardware upon which the files reside is not protected, accessed by consent, and/or by means of a well-founded exception to the Exclusionary Rule of the Warrant Clause. See U.S. Const. amend IV.

Across the United States, a substantial portion of modern-day criminal prosecution relies heavily on ESI residing on computer hardware devices. See "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" (U.S. Dept. of Justice) (2009 ed.) found at <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf> Accessing ESI on computer hardware implicates both the Fifth and Fourth Amendments to the United States Constitution. As a result, Articles XII and XIV of the Massachusetts Declaration of Rights are likewise triggered.

The act of producing a password to computer hardware is not analogous to compulsion of evidence derived from one's person such as DNA. Recently, this Honorable Court held that defendants failed to show extraordinary circumstances involving irreparable error, so as to be entitled to interlocutory relief

under M.G.L. c. 211 § 3. See *Commonwealth v. Bertini*, 466 Mass. 131 (2013). In *Bertini*, the Commonwealth filed a motion seeking an order to compel defendants indicted for armed robbery (and other offenses) to provide a "buccal swab" for DNA testing. This Honorable Court stated that "...defendants make substantial claims alleging violations of substantive rights, as the taking of a buccal swab implicates 'the protections afforded by the Fourth Amendment to the United States Constitution against unreasonable searches and seizures.'" *Commonwealth v. Bertini*, *supra* at 5 (2013) citing *Commonwealth v. Maxwell*, 441 Mass. 773, 777, 808 N.E.2d 806 (2004). Notwithstanding, the interlocutory review was found unwarranted inasmuch as the compulsion of defendants' DNA—even if by reasonable physical force—did not trigger the superintendence of interlocutory review. See *Id.* ("While the taking of a buccal swab implicates "the protections afforded by the Fourth Amendment to the United States Constitution against unreasonable searches and seizures," it is, without more, not so significant an intrusion as to render the intrusion irreparable through the normal process of appeal." citing *Commonwealth v. Maxwell*, *supra*, and *Maryland v. King*, -- U.S. --, 133 S.Ct. 1958, 1978, 186 L.Ed.2d 1 (2013) (quoting *Bell v. Wolfish*, 441 U.S. 520, 557, 99 S.Ct. 1861, 60 L.Ed.2d 447 (1979)) ("expectations of privacy of an individual taken into police custody 'necessarily [are] of a diminished scope'").

Compelling a criminal defendant to provide the government with a password to a lawfully seized encrypted piece of computer hardware poses a *serious threat* on not only Defendant-appellant's Fifth Amendment right against self-incrimination, but also those of other potential members of society across the Commonwealth of Massachusetts who may be similarly situated. Unlike a blood sample or buccal swab for DNA testing, compelling a criminal defendant to produce to the government a computer password forces a defendant to "speak," thereby enabling the Commonwealth to not only break the constitutional right to silence, but also to permit the use of derivative evidence not otherwise proactively proffered by the defendant.²⁰

First, enabling the government to seek leave of Court to compel a defendant to produce a password violates well-settled United State Supreme Court precedent concerning the "Act of Production" privilege established by *Fisher v. United States*, 425 U.S. 391 (1976).

²⁰ Although the question is not raised, Amici respectfully alert this Honorable Court to the fact that compelling the production of a computer password to the government would essentially force a criminal defendant to bypass his or her legal counsel and "speak" to the prosecution. Therefore, it is very probable compelling the production of any information requiring the *eliciting of statements* will violate a defendant's right to counsel under the Sixth Amendment to the United States Constitution as well as under the Fifth Amendment. See *Massiah v. United States*, 377 U.S. 201 (1964).

The constitutional concerns regarding protection of ESI under the Fifth Amendment are the same as those applicable when a defendant is the subject of a criminal investigation and there is a question as to whether the subject should voluntarily speak to law enforcement officials, knowing that such statements may be used against the individual. See *Schneckloth v. Bustamonte*, 412 U.S. 218 (1973) (holding voluntariness determined under totality of circumstances test). Compelling a defendant to furnish a password to his or her computer is tantamount to compelling the defendant to waive an act of production privilege, thereby tainting the voluntariness of the act.

In *United States v. Buckner*, 407 F. Supp. 2d 777 (W.D. Va. 2006), the Court held that the defendant's wife could validly consent to a search of the family computer, including her husband's password-protected files. The Court distinguished *Trulock* because the computer was leased by the wife and the allegedly fraudulent activity catalyzing the search occurred through accounts in the wife's name. In addition, the computer subject to the search was located in a common area of the home, none of the files residing on the system were encrypted, and the computer was on, even though the husband had apparently fled the area. See *Id.* at 780-81.

III. Society Has Adopted An Objective Expectation Of Privacy In Computer Passwords And Encrypted Data Protected By The Fourth Amendment Of The United States Constitution And Article 14 Of The Massachusetts Declaration Of Rights.

The Fourth Amendment to the United States Constitution and Article 12 of the Massachusetts Declaration of Rights protect individuals from unreasonable governmental searches and seizures. A fundamental principle of due process is that all individuals enjoy a reasonable expectation of privacy surrounding their person and personal effects. This includes ESI as well as tangible property. The due process principle is triggered whenever the government oversteps its bounds and improperly seizes evidence.

The issue of compelling a defendant to furnish a password to access otherwise encrypted ESI raises Fourth Amendment issues in addition to those under the Fifth Amendment set forth above. Notably, it is unlawful in the Commonwealth for one to gain unauthorized access to a computer system. See M.G.L. c. 266 § 120F.²¹ Therefore, it is arguably apparent that legislative

²¹ M.G.L. c. 266 § 120F reads as follows:

§ 120F. Unauthorized Accessing of Computer Systems;
Penalty; Password Requirement as Notice.

Whoever, without authorization, knowingly accesses a computer system by any means, or after gaining access to a computer system by any means knows that such access is not authorized and fails to terminate such

intent exists to keep access to a computer subject to prior consent or authority. Compelling a criminal defendant—or otherwise imposing the burden upon him or her—to produce a password for the government to gain access to ESI also implicates a serious potential for a Fourth Amendment violation. It is clear the Massachusetts Legislature intended a heightened level of privacy be afforded data protected by password. *Id.* (stating “The requirement of a password or other authentication to gain access shall constitute notice that access is limited to authorized users”).

Permitting the Commonwealth to demand passwords to encrypted data would result in a *per se* violation of an individual’s right to privacy. This position is supported by the legislative intent to classify password-protected data as inherently private. See M.G.L. c. 266 § 120F (The requirement of a password or other authentication to gain access shall constitute notice that access is limited to authorized users.)

The privacy protections afforded oral and written communications, depending on the environments in which they occur, have been determined by American jurisprudence to be

access, shall be punished by imprisonment in the house of correction for not more than thirty days or by a fine of not more than one thousand dollars, or both.

objectively reasonable. See *Katz v. United States*, 389 U.S. 347 (1967). DNA, for example, does not enjoy the level of protection provided to a defendant's own testimonial statements.

Recently, in *Maryland v. King*, the United States Supreme Court held that when officers make an arrest supported by probable cause to hold a suspect for a serious offense, the government has the right to detain the individual in custody and take and analyze a cheek swab of the arrestee's DNA. See *Maryland v. King*, 133 S. Ct. 1958 (2013). The Court analogized the process to fingerprinting and photographing and, therefore, categorized DNA analytics of an arrestee to a legitimate police booking procedure that is reasonable under the Fourth Amendment. See *Id.*

However, as technology changes, arguably so should the manner in which courts across the United States apply the two-factor "subjective/objective" test expounded by the U.S. Supreme Court in *Katz v. United States*. In a concurring opinion, Justice Harlan built upon the foundations of the majority opinion and formulated the "reasonable expectation" test for determining whether government activity constitutes a search. Harlan's test, not the majority opinion, is the most common formulation cited by courts. Later, this test was arranged into a two prong test for determining the existence of privacy: If (1) the individual "has exhibited an actual (subjective) expectation of privacy," and (2) society is prepared to recognize that this expectation

is (objectively) reasonable, then there is a right of privacy in the given circumstance. This test was adopted by the majority in *Smith v. Maryland*, 442 U.S. 735 (1979), *Katz v. United States*, 389 U.S. 347 (1967)

In *Skinner v. U.S.*, the United States Court of Appeals for the Sixth Circuit held, *inter alia*, that Skinner did not have a reasonable expectation of privacy in the geo-location data produced by the mobile phone that became available to law enforcement officials from the cell phone carrier's network. Notwithstanding whether one agrees with the Court's rationale in *Skinner*, it is nonetheless a good example of how the information residing or produced by a computer device available through a third party (e.g., a cell phone carrier, internet service provider, etc.) does not rely upon the defendant him or herself providing the access. See *Fisher v. United States*, 425 U.S. 391 (1976).

Therefore, like cell phone content accessible through a third party, DNA is not inherently private inasmuch as it can be recovered from physical objects discarded by the defendant (e.g., clothing, cigarettes, etc.). A computer password, if kept private, cannot be recovered from a source beyond the defendant himself.

CONCLUSION

For the reasons set forth herein above, *Amicus Curiae* respectfully request this Honorable Court hold that a defendant must not be ordered to compel an undisclosed password to a lawfully encrypted computer.

Respectfully submitted,

FOR AMICI CURIAE,

August 23, 2013



Daniel K. Gelb (BBO# 659703)
GELB & GELB LLP
84 State Street
Boston, MA 02109
(617) 345-0010 (T)
(617) 345-0009 (F)
dgelb@gelbgelb.com

Daniel B. Garrie, Esq.
LAW & FORENSICS
Senior Managing Partner
6506 3rd Ave NW, Suite C
Seattle, WA 98117
(215) 280-7033 (T)
daniel@lawandforensics.com

APPENDIX A

(Description of Amici Curiae)

Daniel K. Gelb, Esquire
GELB & GELB LLP

Daniel K. Gelb, Esq. is a partner at the law firm of Gelb & Gelb LLP in Boston, Massachusetts. Mr. Gelb represents clients in general and white collar criminal defense matters, complex civil litigation focusing on business and securities, as well as in arbitrations and regulatory proceedings. Prior to joining Gelb & Gelb LLP, Mr. Gelb was an Assistant District Attorney with the Norfolk County District Attorney's Office in Massachusetts.

Among various other professional affiliations, Mr. Gelb is a member of the Advisory Board for Bloomberg BNA's *White Collar Crime Report*; the National Association of Criminal Defense Lawyers' White Collar Crime Committee; and The Sedona Conference® Working Group on Electronic Document Retention & Production.

Mr. Gelb is a frequent speaker and author on electronic discovery and other subject matters impacting both civil and criminal trial practice and procedure. Mr. Gelb has been published by various media outlets including Bloomberg BNA's *White Collar Crime Report*, *Criminal Law Reporter*, and *Digital Discovery & e-Evidence*®. Mr. Gelb has also authored articles published by *Corporate Counsel Magazine*, National Association of Criminal Defense Lawyers' *The Champion*, and *Criminal Justice Magazine* published by the American Bar Association.

Mr. Gelb is the co-author of the book *Massachusetts E-Discovery & Evidence: Preservation Through Trial* published by Massachusetts Continuing Legal Education, Inc. and is a contributing author to *Dispute Resolution & e-Discovery* published by Thomson Reuters WESTLAW.

Mr. Gelb is admitted to practice law in the Commonwealth of Massachusetts, State of New York as well as before the United States District Court for the District of Massachusetts and the United States Court of Appeals for the First Circuit. Mr. Gelb received his B.A. in English from Tufts University; J.D. from Boston College Law School; and M.B.A. from Boston College.

Daniel B. Garrie, Esquire
LAW & FORENSICS, INC.

Daniel Garrie, Esq. is the Senior Managing Partner to Law & Forensics LLC, a boutique legal consulting firm headquartered in Seattle with satellite offices in California, Delaware, Georgia, Missouri, New York, North Carolina, and Brazil.

Law & Forensics works with clients across industries to address cyber security, e-discovery, and digital forensic issues in the U.S. and abroad. Our team has worked on over 1000+ forensic, data breach, and e-discovery disputes all over the world. Our team has also been cited in Forbes, Wall Street Journal, Daily Journal, and Wired Magazine on cyber security, e-discovery, and forensic issues.

Mr. Garrie is a renowned e-discovery and computer security attorney and forensic neutral, e-discovery special master and is a recognized thought leader in the fields of computer software design, cyber warfare, information security, digital forensics, e-discovery, information governance, and digital privacy. Quoted in Forbes and profiled in the Los Angeles Daily Journal. Mr. Garrie is a member of the International Institute for Conflict Prevention and Resolution (CPR) Panel of Distinguished Neutrals; a Neutral on the Hong Kong International Arbitration Centre; Chair of the Forensic and E-Discovery Panel at Alternative Resolution Centers; and an Arbitrator with the London Court of International Arbitration neutrals. In addition, Mr. Garrie has served as an Electronically Stored Information Liaison, Forensic Neutral and Computer Expert for the L.A. Superior Courts, 2nd Circuit, 3rd Circuit, 7th Circuit, New York Supreme Court, and Delaware Supreme Court. In the past two years, Mr. Garrie has been involved in hundreds of computer forensics, breach investigation, and e-discovery matters both in the U.S. and abroad. In addition, Mr. Garrie has advised several global banks and energy firms on e-discovery, information governance, cyber security, and privacy initiatives.

Mr. Garrie is currently the Editor in Chief of the *Journal of Law & Cyber Warfare*, a fellow at the Ponemon Information Privacy Institute, and on the Organization of Legal Professionals board of governors. He has published over 100 articles and is recognized by several Supreme Court Justices for his legal scholarship and is lectures around the world, including recently for the 7th Circuit Pilot Program on e-Mediation with Judge Nan Nolan.

Mr. Garrie also co-authored the treatise *Dispute Resolution and e-Discovery* and another one to on *Software and the Law* both are published by Thomson Reuters.

Mr. Garrie is admitted to practice law in Washington State and New York.

National Association of Criminal Defense Lawyers

The National Association of Criminal Defense Lawyers (NACDL) is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct.

NACDL was founded in 1958. It has a nationwide membership of approximately 10,000 and up to 40,000 with affiliates. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers. The American Bar Association recognizes NACDL as an affiliated organization and awards it representation in its House of Delegates.

NACDL is dedicated to advancing the proper, efficient, and just administration of justice including issues involving the Fifth and Fourth Amendments to the Constitution of the United States and similar provisions contained in state constitutions. NACDL files numerous amicus briefs each year in the U.S. Supreme Court and other courts, seeking to provide amicus assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole.

NACDL has a particular interest in this case because it raises important issues involving the application of Fifth Amendment and Fourth Amendment principles to a modern technology that is relied upon by a large and growing population of citizens. The issues raised in this case involve fundamental questions about the scope of the right to privacy and the right to be free from self incrimination as guaranteed by the Fourth, Fifth and Fourteenth Amendments to the United States constitution and Article 12 and 14 of the Massachusetts Declaration of Rights.

APPENDIX B

Federal Constitutional Provisions:

Amendment IV. 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.

Amendment V. No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Amendment VI. In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the assistance of counsel for his defense.

Massachusetts Constitutional Provisions:

Article XII. No subject shall be held to answer for any crimes or offence, until the same is fully and plainly, substantially and formally, described to him; or be compelled to accuse, or furnish evidence against himself. And every subject shall have a right to produce all proofs, that may be favorable to him; to meet the witnesses against him face to face, and to be fully heard in his defense by himself, or his council at his election. And no subject shall be arrested, imprisoned, despoiled, or deprived of his property, immunities, or privileges, put out of the protection of the law, exiled, or deprived of his life, liberty, or estate, but by the judgment of his peers, or the law of the land.

Article XIV. Every subject has a right to be secure from all unreasonable searches, and seizures, of his person, his houses, his papers, and all his possessions. All warrants, therefore, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation; and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure: and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws. [See Amendments, Art. XLVIII, The Initiative, II, sec. 2].

Massachusetts Statutory Provision:

Section 120F [of M.G.L. c. 266]. Whoever, without authorization, knowingly accesses a computer system by any means, or after gaining access to a computer system by any means knows that such access is not authorized and fails to terminate such access, shall be punished by imprisonment in the house of correction for not more than thirty days or by a fine of not more than one thousand dollars, or both.

The requirement of a password or other authentication to gain access shall constitute notice that access is limited to authorized users.

MASS. R. A. P. 16(K) CERTIFICATION

The undersigned hereby certifies that the above complies with the rules of court that pertain to the filing of briefs, including, but not limited to: Mass. R. A. P. 16(a) (6); Mass. R. A. P. 16(e); Mass. R. A. P. 16(f); Mass. R. A. P. 16(h); Mass. R. A. P. 18; and Mass. R. A. P. 20



Daniel K. Gelb

CERTIFICATE OF SERVICE

I, Daniel K. Gelb, Esquire do hereby certify that on August 23, 2013 I served two (2) copies of the above amicus brief by U.S. Mail on the following counsel of record for the above-captioned parties:

For Defendant-Appellant Leon Gelfgatt:


STANLEY HELINSKI, ESQUIRE
HELINSKI LAW OFFICES
ONE MCKINLEY SQUARE
BOSTON, MASSACHUSETTS 02109

PAUL J. DAVENPORT, ESQUIRE
HELINSKI LAW OFFICES
ONE MCKINLEY SQUARE
BOSTON, MASSACHUSETTS 02109

For Commonwealth-Appellee:

RANDALL E. RAVITZ, ASSISTANT ATTORNEY GENERAL
OFFICE OF THE MASSACHUSETTS ATTORNEY GENERAL
CRIMINAL BUREAU
ONE ASHBURTON PLACE, 18TH FLOOR
BOSTON, MA 02108

JOHN P. ZANINI, ASSISTANT DISTRICT ATTORNEY
OFFICE OF THE SUFFOLK COUNTY DISTRICT ATTORNEY
ONE BULFINCH PLACE
BOSTON, MA 02114



Daniel K. Gelb