C13 Implications for Digital Forensics Investigations of the United States 2nd Circuit Ruling Upholding Deletion of Non-Responsive Computer Files: A United States and European Union/Germany Perspective

Donald J. Horowitz, JD, c/o 4311 11th Avenue, N, Seattle, WA 98105; Barbara E. Endicott-Popovsky, PhD, 4311 11th Avenue, NE, Ste 400, Seattle, WA 98105; Aaron Alva, 2001 E Yesler Way, #33, Seattle, WA 98122; Hellen Schiling, PhD, Kempf & Dannenfeldt, Siesmayerstraße 58, Frankfurt am Main 60323, GERMANY; Carsten Rudolph, PhD, Fraunhofer SIT, Institute for Secure Information, Technology, Darmstadt, GERMANY; and Nicolai Kuntze, Rheinstrasse 75, Darmstadt, Hessen 64295, GERMANY*

The goals of this presentation are to discuss ruling impacts and to describe current research in the United States and the European Union/Germany addressing selective suppression.

After attending this presentation, attendees will better understand the results of research into technical and legal issues arising from this landmark decision. This has significant technical and legal implications for all digital forensics investigations.

In *United States v. Ganias*, June 2014, the Second Circuit held that the government has a duty to delete or return non-responsive data it had previously seized through a valid search warrant, raising the bar for what the government must do post-seizure of digital evidence.[1] Attendees will learn the results of this research into technical and legal issues arising from this landmark decision. This has significant technical and legal implications for all digital forensics investigations.

This presentation explores the implications of this ruling from the technical and legal perspectives of experts in the United States and the European Union and of members of a digital forensics research collaboration between the University of Washington and Fraunhofer Institute Darmstadt. This study also discusses comparative selective suppression procedures used in Germany.[2-5]

Technology and policy are often on a collision course; this ruling is an example. The technical challenges are many: (1) how do we delete non-responsive data from disk images without violating the integrity of responsive files; (2) what do we do with hash values and digital signatures; (3) how do we edit video and audio files to show that all retained parts correspond to their respective parts from the original file; (4) how do we create signatures that show which parts were deleted; and, (5) how do we delete parts of a database without violating relevant data or complete databases with mainly non-responsive information that might not be retained at all?

Additional legal/policy concerns include: (1) what procedures will the government use to delete non-responsive data; (2) whose responsibility will it be to perform the deletion; (3) must the government verify the deletion and, if so, how can the deletion be verified; (4) how long can a non-responsive file be retained before it becomes an unreasonable seizure; (5) how does this interact with rights that criminal defendants have on appeal; (6) what is considered a "document;" and, (7) who decides what is non-responsive?

Although the government argued that selective deletion from an imaged hard drive would be impractical, the court stated that it was not entirely convinced: "But even if we assumed it were necessary to maintain a complete copy of the hard drive solely to authenticate evidence responsive to the original warrant, that does not provide a basis for using the mirror image for any other purpose." This begins to imply what the court thinks authenticity may entail, but raises the additional questions described above.

Similar to the United States, in Germany, infringement due to search-and-seizure measures is justified only on the condition that they are in accordance with the German Criminal Procedure Code, securing data always requires the object in question to be of significance for the investigation.[6] To determine evidentiary significance, off-site reviews are permitted pursuant to the German Criminal Procedure Code.[7] As soon as a decision is made, these documents/data must be returned or deleted; however, German authorities recognize that selective suppression was "impractical," respectively "technically impossible," due to harming the validity of a mirror image.[1]

In contrast, securing storage media in Germany is enshrined in the constitutionally guaranteed "right on informational self-determination" and the "guarantee of the confidentiality and integrity of IT-systems"; both rights derive from the general "right of freedom" in connection with the "guarantee of human dignity" of the German Basic Law.[8,9]

This study explores the technical and legal research on selective suppression. While the technical team explored a technical solution to the questions raised in this presentation, it was discovered that German procedures for off-site review and their views on rights regarding digital information have relevance to questions raised by the 2nd Circuit decision.[1] These will be discussed and reviewed anticipating that the discoveries and insights in this study may be helpful to those adapting their digital forensics investigations to updated decisions.

References:

1. Orin Kerr (@OrinKerr)6/18/14, 0:09: Second Circuit adopts a 4th Am right to the deletion of non-responsive computer files. A hugely important case. *washingtonpost.com/news/volokh-co…*
2. Dardick, G., Endicott-Popovsky, B., Gladyshev, P., Kemmerich, T., Rudolph, C. (2014). Digital Evidence and Forensic Readiness. Dagstuhl Seminar 14092.
3. Rudolph, C., Kuntze, N., Manz, D., Endicott-Popovsky, B. (2014) Do I Trust You? A Discussion on Trust, Security and Internet-connected Devices Today and Tomorrow. International Workshop on Engineering Cyber Security and Resiliance (ECSaR'14), 31 May, Stanford, CA.
4. HRRS-publication (HRRS 2013, 207, available on www.hrr-strafrecht.de)
5. Kuntze, N. Rudolph, C., Schilling, H., Alva, A., Brisbois, B., Endicott-Popovsky, B. (2014) Seizure of digital data and "selective wuppression" of digital evidence. Paper presented at 8th International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE) at IEEE/International Conference on Digital Forensics and Cyber Crime, New Haven, Connecticut. (TBD).
6. Sec. 94 of the German Criminal Procedure Code
7. Sec. 110 of the German Criminal Procedure Code
8. Art. 1 par.1 and Art 2 par. 1 of the German Base Law
9. Art. 13 of the German Base Law

2nd Circuit Ruling, Selective Suppression, Digital Forensics