Brendan Francis O'Connor

1813B S King St.
Seattle, WA 98144
406-545-0430
bfo@ussjoin.com

November 22, 2016

Ed Smith
Clerk of the Montana Supreme Court
Room 323, Justice Building
215 N. Sanders
Helena, MT 59601

Re: AF 09-0688 - Addition of Rule 4.4(c) to the Rules of Professional Responsibility

Honorable Justices of the Montana Supreme Court,

My name is Brendan Francis O'Connor. I am an attorney admitted to practice in the State of Montana; I am also a researcher and practitioner in the field of computer security.[1] I write to comment from a technical perspective on the proposed addition of a Rule 4.4(c) to the Montana Rules of Professional Responsibility, the text of which is as follows:

> "A lawyer shall not knowingly access or use electronically stored information in a communication or document received from another lawyer, for the purpose of discovering protected work product, privileged or other confidential information unless the receiving lawyer has obtained permission to do so from the author of the communication or document. Communication or document as used in this rule excludes documents produced in discovery and information that is the subject of criminal investigation."

First, **the rule, as drafted, does not produce a workable distinction between "electronically stored information" and the content of a document—nor does one exist.** It seems likely, from the phrase "electronically stored information *in* a communication or document" that the drafters mean any information that was not typed

[1] I hold the degrees of Bachelor of Science in Computer Science and Master of Science in Engineering in Computer Science from The Johns Hopkins University. While I was in law school, I pursued, was awarded, and successfully completed two research contracts, awarded by the United States Defense Advanced Projects Research Agency (DARPA) in the field of computer security (DARPA Cyber Fast Track). I have presented technical research at computer security conferences in the United States, Canada, Norway, and the Netherlands; I have also presented at a variety of legal venues in the United States and Europe on both legal and technical issues, including two CLE presentations for the State Bar of Montana. I have served as Vice-Chair of the American Bar Association's Information Security Committee (ST-ISC) since August 2014; however, this comment does not necessarily represent the views of the ABA or of the Committee.

at a keyboard by a human being—so-called "metadata." The issue with restricting document metadata is that there is not a meaningful difference between content and metadata—all of the data in a file is interpreted and used by standard tools in their normal course of operation.

For instance, take the case of a JPEG image.[2] A digital camera is simply a computer with a specialized light sensor on it.[3] When the camera takes a picture, the sensor captures light during the instant that the shutter is open. Once the light has been captured in a temporary format stored in the computer's memory, the computer adds a large amount of information to the photo to allow it to be interpreted by other computers before saving it. This information, called EXIF data,[4] often includes the model of camera, the lens used, whether the flash was triggered, the focal length and aperture setting of the camera, and information necessary to display the image (for instance, information about how color is represented in the image, or the image rotation). The information can be very extensive; it may include the serial number of the camera, the location, altitude, and direction of the camera,[5] and information about how the photo was edited, if the photo was edited at the time it was taken (on the camera) or later (e.g., using Adobe Photoshop).

This information does not require deep technical understanding to locate or use; indeed, every image-displaying program will need at least some of the information, and common image software, from Photoshop or iPhoto to the Flickr image-sharing website, will make great use of all of the EXIF data. For instance, Flickr's mapping functionality[6] automatically places images uploaded to it on a world map; this allows people to look in specific areas for photos of interest. One might search "court" near 59620 and find images of the Old Supreme Court Chamber; these would be different from searching "court" near 59101 and finding images of Billings courthouses. Similarly, many "photo album" programs automatically use the image location to categorize different parts of a trip. In this way, the location is not separate from the image; it is a significant part of understanding the image and being able to work with it efficiently, and that is why it is included in the image file. The same is true for all of the information embedded in the image, from the color of a part of the image to the lens used to capture the image. Indeed, Flickr displays nearly all this information for each image when a user clicks

[2] JPEG stands for the Joint Photographic Experts Group, a standards body that created the JPEG image standard (as well as several revisions and extensions). The JPEG format is commonly used for photos. Files in JPEG format often have the filetype ".jpeg" or ".jpg."

[3] Indeed, camera manufacturers speak openly about the importance of the signal processing and other functions of the computers they attach to the light sensor. See, e.g., http://www.learn.usa.canon.com/resources/articles/2012/digic_processors.shtml .

[4] Exchangeable Image File format data (EXIF data) is used with a variety of image formats, including JPEG.

[5] Position sensors are more common in higher-end cameras; however, smartphones have made the sensor package that captures location and direction so easily obtainable that these features are becoming more common in consumer cameras. In addition, many modern smartphones will capture location information and add it to their images by default.

[6] https://www.flickr.com/map

"Show EXIF," and most software can display relevant metadata for a file being edited in just a few clicks.

Every type of computer file has metadata of one sort or another. Video DVDs contain region and video encoding information, stating where they are meant to be played and how the video is stored. Documents in Microsoft Word format include metadata relating to formatting (selecting the font size, for instance), metadata relating to the document's creator and editors, and in some cases (when the feature has been expressly enabled for a particular document by its creator, for this is not the default), information about changes made to the document. MP3 files include information about the artist and album, as well as information relating to where the music was purchased. Computers store metadata for every file stored on a drive, including when the files were first saved, last changed, and last opened. Even computer hardware has metadata; when a USB device is plugged into a computer, it identifies itself to the computer to explain what it is and how to use it before any other data is transmitted. All of this information is viewable; it does not require special tools or uncommon skills to use. Metadata is inextricable from the normal use and function of any computer. In this way, metadata gives new life to "the medium is the message;" without the metadata to give context to the remainder of the message, it would be unintelligible.

Second, **attorneys already have effective, built-in tools to remove unnecessary metadata from documents**. When attorneys need to remove information from a paper document (for instance, in response to Rule 1.6), they can redact it. Attorneys are also able to remove metadata from a document trivially, if they feel that the metadata might reveal privileged or work product information. For instance, Microsoft Word has several built-in tools to do this, including the "Check For Issues" button prominently displayed in modern versions of Word; in addition, saving the document as a PDF before sending it removes Track Changes, Comments, and many other potential sources of privileged or work product information from a document. These tools are built-in to many document editors and operating systems, and are easy to use when necessary.

Finally, **this rule may have the unintended effect of dissuading Montana attorneys from using technology to manage their legal practices**. Modern legal practice management tools automate the discovery and use of document metadata. For instance, the MetaJure platform[7] uses document metadata, both that which is stored inside the document and that which is found outside the document (such as information about an email to which a document was attached) to locate, organize, and make documents available throughout a firm. This use of metadata helps firms comply with their obligations to their clients and to opposing counsel, by minimizing the number of documents that are lost in the virtual shuffle.

[7] http://metajure.com/

The proposed rule would require that attorneys go to significant lengths to avoid any inadvertent contact with document metadata, lest normal tools for photo viewing, document editing, or the like (all of which *must use and display metadata as part of their normal course of operation*, as described above) reveal confidential information that was transmitted to them. While it is certainly possible that this use might be found not to be "*for the purpose* of discovering… confidential information," the rule will create a chilling effect that dissuades attorneys from using technology to its fullest extent lest they be found to have violated the rule. This is particularly egregious because Rule 4.4(b), which deals with information inadvertently sent to an attorney, does not require this level of care with paper documents; as amended by this Court on September 22, 2016, the rule only requires notification of the sender if an attorney knows that a document was inadvertently sent. To say that electronic documents are somehow both different from paper documents, and more dangerous, significantly harms the cause of efficiency in moving to an electronic practice, which in turn will hurt both clients and the efficient administration of justice.

I recognize and applaud the hard work of the State Bar of Montana on issues relating to technology. I am very much in favor of the change to the Preamble to the Montana Rules of Professional Conduct, adopted by this Court's order on September 22, 2016: "Competence implies an obligation to keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." I think that it is excellent that the Bar and the Court wish to ensure that the Rules take into account the changing nature of technology; when they do so, it would be my request that they first ask if their goals are best met by curtailing a particular use of technology, or by, as in the Preamble, reaffirming an attorney's existing obligations regardless of the medium. In many cases, I would submit that the answer most in keeping with the tenor and traditions of the legal profession would be the latter.

I humbly request that this Court reject the proposed Rule 4.4(c) in its entirety.

Sincerely yours,

Brendan Francis O'Connor

Brendan Francis O'Connor