Attorney Advertising

Robinson+Cole

Intelligence

**TRENDING**

## Applying Old Laws to New Technologies: The Challenges of Regulating Cryptocurrencies

In the past several months, cryptocurrencies have been all over the news with the meteoric rise in the value of Bitcoin up to $20,000. At its peak in early January 2018, the total market capitalization of all cryptocurrencies approached $800 billion before dropping to below $300 billion by April as Bitcoin's value fell precipitously. These extreme fluctuations in value, paired with numerous examples of fraud and criminal activity, naturally raise the question of government regulation. So who is responsible for regulating this rapidly expanding industry? The answer depends on how cryptocurrencies are classified.

Cryptocurrencies (or virtual currencies) such as Bitcoin, Litecoin, and Ether, are digital representations of value maintained in decentralized databases secured by encryption known as a blockchain. Cryptocurrencies can be used as a medium of exchange, but are not backed by the government or other commodities. There are now hundreds of different cryptocurrencies available, with many being offered through Initial Coin Offerings (ICOs), in which projects raise funds by selling their crypto tokens to the public. These ICOs have been a frequent target of hackers and fraud, heightening concerns about the practice.

With no comprehensive federal law regulating cryptocurrencies, multiple federal agencies have asserted jurisdiction over the industry. The Securities Exchange Commission (SEC) considers most cryptocurrencies, particularly those offered through ICOs, to be **securities** subject to regulation and registration requirements. The Treasury Department's Financial Enforcement Network (FinCEN) treats cryptocurrencies as a form of **money**. The Commodity Futures Trading Commission (CFTC) declared that cryptocurrencies are **commodities**, and a recent decision by the United States District Court for the Eastern District of New York upheld that interpretation, recognizing CFTC's standing to regulate virtual currencies under the Commodity Exchange Act.

Rather than adopt a one-size-fits-all regulatory classification, Wyoming recently adopted legislation differentiating between cryptocurrencies marketed as investments and those that actually are used as a medium of exchange for goods, services, or content. Under Wyoming's new law, the latter category, referred to as "utility tokens,"

**Q2 2018**

---

**FEATURED TOPICS**

**TRENDING**
Regulatory
Cryptocurrencies

**GC SURVIVOR KIT**
Work Made For Hire

**SPOTLIGHT**
Health Care IT - Information Blocking

---

**FEATURED AUTHORS**

Nathaniel T. Arden
Alaine C. Doolan
Benjamin C. Jensen
Jacqueline P. Scheib

is exempted from state securities and money transmitter laws and is treated as a new class of asset.

In the absence of Congressional guidance, federal agencies and the states will continue to attempt to use existing laws and guidance to regulate the industry. The ultimate determination of how to classify cryptocurrencies will have far-reaching taxation, registration, and licensing impacts on business and market participants and could significantly shape how this emerging industry develops in the United States.

---

**GC SURVIVOR KIT**

**Work Made For Hire. It's Not What You Think.**

ABC Co. (ABC) hires Joe to develop a computer program. ABC designs the specifications for the software, tests the software, supervises the modifications Joe makes, and pays Joe $100,000 for his efforts. After the software has been installed on ABC's system, ABC learns that Joe has been marketing ABC's program and has already sold it to XYZ Co., ABC's biggest competitor, for just $25,000. Can ABC stop Joe?

The above scenario happens more than you might think. It is natural to assume that because you engaged and paid someone to create something for you, that you would have ownership rights in that creation. However, this assumption is often incorrect. Ownership of copyrighted works is particularly important because owners of copyrighted works have the exclusive right to reproduce the work, prepare derivatives from the work, distribute copies of the work to the public, perform the work publicly, display the work publicly, and authorize others to exercise these exclusive rights. To ensure your ownership, the work must be either created as a "work made for hire" or transferred to you through an effective written assignment.

Under the U.S. Copyright Act, ownership of a copyright to a work generally belongs to its author unless it meets the requirements of a "work made for hire." The U.S. Copyright Act provides that a work made for hire exists only if (1) the work is prepared by an employee for his/her employer within the scope of employment; or (2) the work is specially ordered or commissioned, falls within one of nine very specific categories of work, and has been assigned through a written agreement. If "work made for hire" does not apply, the creator of the work is the sole copyright owner and alone holds the exclusive rights to the work. Unless these rights are assigned to the commissioning party, the author has control over the work and can even prevent the commissioning party from reproducing or modifying it.

**The Employer-Employee Relationship**

A key component of the work made for hire doctrine is establishing an employer/employee relationship. Determining whether a person is an employee can sometimes require the weighing of multiple factors including, without limitation, the following:

- Supervision and Control – Who controls the flow of the work, and who supervises the creator's development efforts?
- Control Over the Work – Who determines how the work is done, where it is done, and what resources, equipment, or supplies have been provided to create the work?
- Overall Context – Is the party who commissioned the work in the business of producing such works? Are the services part of the engaged individual's regular service obligations? Is the engaged individual receiving benefits, salary, and/or are employment taxes withheld from the engaged person's payments?

**Scope of Employment**

Another key element of the "work made for hire" doctrine is whether the work was created by an employee within his/her usual "scope of work." In other words, do the tasks that an employee is responsible for include development of the work? For example, if Joe from our scenario above is hired as a salaried employee with benefits and his job description is a software developer, then the work would likely fall within the scope of work made for hire, and the employer would own the copyright to the software that Joe developed.

**Specially Commissioned Works**

"Work made for hire" can also attach to the following narrow categories of specially ordered or commissioned work: (a) contributions to a collective work, part of a motion picture or other audiovisual work, (b) as a translation, (c) as a supplementary work, (d) as a compilation, (e) as an instructional text, (f) as a test, (g) as answer material for a test, or (h) as an atlas. In each of those cases, the parties also must agree, in writing, before the work is created, that the resulting work will be a "work made for hire" even though the creator is not an employee of the commissioning party. In this situation, the copyright would be owned by the commissioning party.

**The Bottom Line**

Most of the time – but not all of the time – work developed by employees will be owned by the employer without the need for a written assignment. Works developed by non-employees will never be owned by the engaging party unless a written assignment is in place, even if they are engaged to create one of the categories of specially commissioned works identified in the "work made for hire" doctrine.

As a precaution, it is always a good idea to have any person involved with development of intellectual property and/or technology sign a written agreement with language stating that if the developed work is not recognized under the law as a "work made for hire," then the individual assigns all rights, title, and interest to you in his/her developed works, ideas, creations, and inventions conceived or created during the course of the engagement by you.

**SPOTLIGHT: ON HEALTH CARE IT**

**Health Information Technology Community Awaiting Much-Needed Proposed Rule**

Late last year, the Office of National Coordinator for Health IT (ONC) announced that it expected to release a proposed rule in the Spring of 2018 that would provide clarity to the health care industry about the meaning of "information blocking," as defined in the 21st Century Cures Act (the "Cures Act"). The Cures Act was signed into law in 2016 and included provisions preventing health care providers from engaging in information blocking. Ever since, providers and information technology vendors, information exchanges, and networks (collectively, "health IT vendors"), particularly electronic medical record (EMR) vendors, have been trying to decipher the law's meaning to avoid the potentially massive fines associated with information blocking (up to $1 million per violation).

The Cures Act defines information blocking as a practice that is likely to interfere with, prevent or discourage access to, or exchange or use of, electronic health information. A health IT provider may not engage in information blocking if it "knows or should know" that such action is likely to interfere with, prevent or materially discourage access to, or exchange or use of, electronic health information. Providers are given more leniency through the incorporation of a knowledge standard. Specifically, providers are prohibited from engaging in information blocking if the provider "knows" that its actions are unreasonable and likely to interfere with, prevent or materially discourage access to, exchange or use of electronic health information. Congress provided a few examples of information blocking, to help clarify the scope of the law, including the following:

- practices that restrict *authorized* access, exchange or use for treatment and other permitted purposes;
- non-standard implementation of health IT in ways that are likely to substantially increase the burden of accessing, exchanging or using electronic health information;
- implementing health IT in ways that are likely to restrict access, exchange or use of electronic health information when exporting information or transitioning between different health IT systems; and
- implementing health IT in a manner that is likely to impede innovations and advancements in accessing, exchanging or using health information.

Congress's goal in enacting the information blocking provisions was to encourage the free exchange of information among providers and to push health IT vendors to develop interoperability standards. However, Congress appears to have created more confusion around information sharing, as many are confused by what constitutes a "likely" interference with, or what it means to "materially" discourage access to information.

Unsurprisingly, many in the health care industry were confused by the Cures Act's information blocking definition and examples, and combined with the potentially large fines, providers and health IT

vendors are concerned about the information blocking law. However, there have been no reported cases of violations of the law or of fines assessed. Most in the industry believe that the ONC and the Department of Health and Human Services Office of Inspector General, which is tasked with enforcing the information blocking prohibitions, are focusing on blatant violations of the law. For example, a health IT vendor building into its EMR system a functionality to prevent exporting information to a rival's EMR system or a provider restricting a patient's ability to send electronic patient records to a non-affiliated provider. Outside of these fairly straightforward instances, the bounds of what may constitute information blocking are unclear. For example: Are providers required to maintain complete interoperability with all other health IT systems with which they interact, regardless of cost or resources required? Is sending a medical record by a PDF or similar format insufficient where it may be technically possible to send a record directly between EMR systems through an interface? Will health IT companies be required to update all of their software to make it completely interoperable with all other EMR systems? What does it mean to implement health IT in a manner that is "likely to impede" innovations? These are only a few of the questions providers and health IT vendors are facing in the wake of the Cures Act. With the ONC's upcoming proposed rule, the health care community is anxiously awaiting clarity.

To further complicate matters, providers participating in Medicare's Merit-based Incentive Payment System (MIPS), which is a method by which Medicare-participating providers are paid for their services to beneficiaries, are asked to attest that they have taken certain actions to prevent information blocking in the provider's practice. Many providers rely on their IT and health information management staff to handle the specifics around implementation of their health IT systems and exchange of medical records. As a result, many of these providers are unsure of the level of investigation they must undertake in order to make an appropriate attestation. The law is also silent on specifics with respect to penalties providers may face for violations; however, the law calls for regulations to specify "appropriate disincentives."

While awaiting the proposed rule, providers, health IT vendors, exchanges and networks would be well-served to review their policies and practices on sharing health information. In particular, providers may want to review their HIPAA-related policies to ensure their practices on sharing patient information are not too restrictive, especially in the case of sharing information with other providers for treatment purposes of a shared patient. Additionally, the proposed rule will include a public comment period, and interested members of the health care community are encouraged to share their comments and concerns with the ONC.

---

**Contributors:**

Jacqueline Pennino Scheib | Nathaniel T. Arden | Alaine C. Doolan

William J. Egan | Benjamin C. Jensen | Andrew W. Monthey | Brian E. Moran

James R. Nault | Kathleen M. Porter | Lisa M. Thompson

For additional information, please contact one of the lawyers listed above or another member of Robinson+Cole's Intellectual Property + Technology Group. For insights on legal issues affecting various industries, please visit our Thought Leadership page and subscribe to any of our newsletters or blogs.