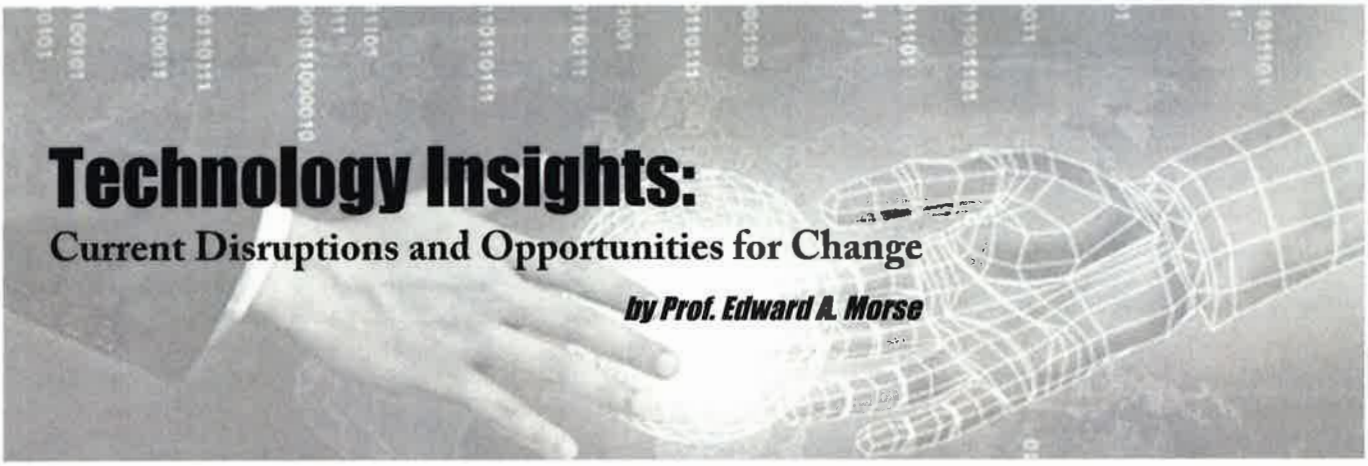

Technology Insights:

Current Disruptions and Opportunities for Change

by Prof. Edward A. Morse

COVID-19 has changed the way we live and work. Social distancing has been foisted upon us to constrain contagion and protect the most vulnerable. We are learning to work apart, moving the locus of our activities away from offices and other public gathering spaces and into our homes. Technologies that make social distancing possible are also fostering changes that will likely endure after the risks of contagion from this virus have subsided. These technologies present challenges and opportunities for our profession and our clients that merit reflection and attention from us as we navigate through this crisis and beyond.

Payments

Payment technologies have long been advancing toward electronic systems and away from paper-based platforms including cash or checks. Paper had a long and successful run. The ancient book of Tobit reports the early use of a paper document to evidence a transferable deposit in a remote land.[1] The parties created duplicate copies of a paper document evidencing the deposit. One copy was torn in two and each counterparty retained half as a means of confirming the identity of one entitled to return of the deposit. In a world with limited duplication technology, tearing created features that could provide a reliable basis for identification of the holder. But woe to the depositor who did not store his half in a mice-proof box.

Paper money issued by sovereign governments continues to provide a reasonably reliable medium of exchange and store of value. Duplicating technologies present counterfeiting challenges, but cash provides a widely accepted and trusted means for payment. Some businesses accept only cash, including "Grounds of Being", the coffee shop at the University of Chicago Divinity School. The proprietors claim that this is "Where God Drinks Coffee", but apparently God should not expect to use an American Express card—or run a tab!

But even before the COVID-19 crisis, some businesses began rejecting cash in favor of electronic payments. These firms recognized that cash presented risks of theft due to its

Prof. Edward A. Morse

Edward A. Morse is a professor of law at Creighton University School of Law where he holds the McGrath North Endowed Chair in Business Law. He frequently speaks and writes on tax and technology. He currently serves as Program Chair for the Cyberspace Law Committee of the ABA, and he expresses gratitude to colleagues there for sharing their insights. He is also the editor of *Electronic Payments: Law and Emerging Technology* (ABA 2018). His faculty webpage can be found here: https://law.creighton.edu/faculty-directory-profile/192/edward-morse.

bearer qualities; disadvantages in transaction speed; and costs and inefficiencies from counting, managing, and moving physical deposits to banks that ultimately convert paper into electronic balances. Governments have also been concerned about cash because of its ability to facilitate criminal activities and tax evasion through anonymous transmissions that frustrate law enforcement efforts.

Cash is king whenever electronic payment networks are affected by natural disaster or terrorism. For example, Federal Reserve banks trucked semi-loads of cash into areas stricken by hurricane Katrina to meet the demand for cash in an environment where ATMs and payment card networks were no longer functioning. Adjustments to check clearing networks were needed when September 11 attacks caused airplanes to be grounded. In contrast, networks remain strong in a pandemic-induced crisis. In this case, cash is no longer king, but instead it becomes a medium for transmitting contagion. The pandemic is likely to nudge us further away from cash, perhaps even toward eliminating its common use.

For the time being, we are safer without cash. But this movement toward safety should also initiate caution about the forms of electronic payments that we choose. Swiping a credit card involves contact with surfaces that are being touched by others. Touchscreens and keypads used to approve an electronic payment may also contain pathogens. Mobile payments and other contactless card payment technologies reduce these contacts and potentially avoid them altogether.

COVID-19 nudges us toward upgrading payment technologies. Payment technology innovation will be driven not only by cost savings generated from avoiding custodial costs for cash, but also from reducing risks of pathological transmission and the costs to sanitize these systems. These concerns will also affect use and acceptance of checks, which present similar concerns about contact and contagion. Some of us have already received notices from clients that bills are to be moved electronically and payments are going to move via ACH or other media in order to protect their personnel. The federal government is wrestling with similar issues as it seeks to deliver benefits from the CARES act to citizens who need them in the most efficient and safe format possible.

Whether we like it or not, our payments and other communications will continue to shift toward electronic media and away from paper. I hope that we do not eliminate the socially gracious practice of handwritten notes to friends and loved ones. I have also heard that giving one's mother-in-law a gift of an ocean cruise might not be viewed as an act of love and kindness. Let us hope that normalcy will return and fear of contact will not cause us to lose those things that we value most. And we should remember that network disruption threats coming from other sources, including natural disasters and terrorism, still lurk in the background for the time being. Sometimes paper can still be our friend, and we should not lose sight of its utility. Shortages in Charmin may be Nature's way of reminding us that our trust in electronics does not always allow us to escape the constraints of the physical world.

Cryptocurrencies: Escaping the Regulated Networks?

Not everyone embraces this movement toward cashless payments. Electronic payments present some tradeoffs, including a potential loss of privacy. You do not have to be a Luddite or a criminal enterprise to have privacy concerns about traditional electronic payment networks. Data collected through payment networks fuel activities such as targeted marketing, credit scoring, fraud prevention, and demand forecasting. But that data also includes evidence of activities that some might prefer to keep private.

Although some view cryptocurrencies as a path to protect one's privacy and particularly to escape the inquiring eyes of the government, they are no panacea.[2] Identities can sometimes be discerned from data gleaned from public ledgers that facilitate cryptocurrency transmission, albeit through applying considerable effort.[3] Market demand has generated new cryptocurrencies that cater to this interest in privacy.

Governments continue to be interested in cryptocurrency regulation and restriction, particularly in controlling funds flowing among criminal enterprises and to other governments subject to economic sanctions. For example, the U.S. Treasury recently announced significant sanctions against individuals acting on behalf of North Korea to launder funds stolen from a cryptocurrency exchange.[4] Cryptocurrency also played a role in efforts to circumvent sanctions on the government of Venezuela.[5]

For most people, the prospects of investigations employing decryption and detective efforts to unmask their cryptocurrency transactions is not a realistic concern. But more easily accessible sources of information are being collected by intermediaries operating entry and exit points to cryptocurrency value chains, which provide a common interface for those seeking to use or acquire cryptocurrency assets. These intermediaries transform sovereign currency into cryptocurrency (or other cryptocurrencies) and vice versa, and their activities are subject to anti-money laundering rules that require collection of personal data on the account holder that may be shared with the government.[6]

The Internal Revenue Service has taken an interest in data from cryptocurrency transactions to ferret out tax avoidance.[7] Cryptocurrency transactions in exchange for goods or services are deemed to involve a disposition of property, which thus presents the possibility of taxable gain.[8] Moreover, even persons who do not exchange cryptocurrency directly for goods and services may also receive taxable income in a

so-called "air drop" following a "hard fork" in the underlying trading platform.[9] Intermediaries have been targeted for information gathering to support tax enforcement efforts. Most notably, Coinbase was the target of a subpoena from the IRS designed to reveal customers with potential cryptocurrency trades and unreported taxable income.[10] The IRS also sent letters to taxpayers designed to educate them about their tax-compliance responsibilities late last year, in advance of the 2020 tax return filing season, thereby sending a strong signal that enforcement efforts are underway.[11] Although the IRS has recently announced that it is "continuing to assess the impact of COVID-19 on a range of compliance activity across the agency,"[12] noncompliant taxpayers likely face audit risks.

Lawyers may have some special responsibilities and concerns in this space. Clients may be interested in using cryptocurrencies for fee payments or for other transactions. Some may do so for benign and legitimate reasons, perhaps because they have exhausted other sources of liquidity during the current crisis. But others may choose this path to avoid those intermediaries that might otherwise be used to convert these currencies to cash, preferring instead to use a channel that has traditionally involved confidentiality and protection from disclosure.

Nebraska lawyers face special ethical duties in this space, which are partly outlined in a Nebraska Ethics Advisory Opinion issued in 2017.[13] That opinion concludes that an attorney may receive digital currencies (another name for cryptocurrencies) such as Bitcoin from a client. However, the attorney must: (1) inform the client that he/she will convert the digital currency into dollars, (2) convert at "objective market rates immediately upon receipt through the use of a payment processor", and (3) credit the client's account at the time of payment.[14] The opinion appears to be rooted in concerns about violating the proscription against unreasonable fees, as conversion freezes the volatility that has historically been present in cryptocurrencies.[15] By converting the currency into dollars, presumably the lawyer and client are able to assess the consideration provided in the familiar and comparatively stable format of the U.S. dollar.

The ethics opinion also allows attorneys to hold cryptocurrencies in escrow or trust for clients or third parties, as long as they are held separately from the lawyer's property and held with "commercially reasonable safeguards." Since cryptocurrencies are property, not sovereign currency, they may not be deposited into client trust accounts pursuant to Neb. Ct. R. §§ 3-901 to 3-907.[16] Thus, the opinion requires a lawyer who receives a cryptocurrency as a retainer must effectively convert it to cash, just as in the case of other fees, and deposit the cash proceeds.

The requirement for security presents real challenges here. Unlike the bank deposit, which is protected against loss from theft or insolvency based on FDIC insurance and other government regulators as well as redundancies in records showing ownership, one keeping cryptocurrency must possess and protect an electronic record known as a "private key" that is critical to transmitting and using that asset. Once that key is lost or compromised, possession is effectively lost and value is destroyed.[17] The opinion suggests one way to protect access might include maintenance of a computer that is disconnected from the internet—so called "cold storage".[18] This may or may not be commercially reasonable under current data security practices, but it is certainly not foolproof. There are rumors of millions of dollars of cryptocurrencies being lost because a hard drive storing the key is damaged or discarded—and it is easy to imagine how that might be possible.

It should be noted that the 2017 Ethics Opinion does not exhaust the ethical and legal questions presented in this environment. Lawyers should also consider the possibility that their role in receiving cryptocurrency and converting them into dollars using their firm account could also facilitate money laundering or tax evasion. Lawyers owe a duty of confidentiality to their clients, which is subject to permissive disclosure in limited circumstances, including prospective commission of a crime.[19] Moreover, lawyers are not permitted to "counsel a client to engage, or assist a client, in conduct that the lawyer knows is criminal or fraudulent."[20]

A permissive disclosure rule involves judgment that balances the public good that comes from confidential communication against the public good from preventing criminal activity.[21] The lawyer's role as gatekeeper in financial networks has been a subject of debate.[22] Legislation has been proposed to expand regulatory measures designed to combat money laundering, and the American Bar Association has gone on record to support "reasonable and necessary domestic and international measures designed to combat money laundering and terrorist financing ... [but] the Association opposes legislation and regulations that would impose burdensome and intrusive gatekeeper requirements on small businesses or their attorneys or undermine the attorney-client privilege, the confidential attorney-client relationship, or the right to effective counsel."[23] State bars will also need to consider how these competing obligations should be balanced, perhaps with enhanced guidance for attorneys in this area.

Data Security: A Heightened Responsibility with Shifting Standards

The trend toward more digital electronic activities and payments highlights the need for enhanced attention to the security of our channels for communication and our means of storing and using sensitive information. Security concerns are familiar to us, as we have been living with embarrassing and destructive impacts of data breaches for some years now.

By shifting operations toward remote workplaces, we may find that sensitive files and information are moving more often. Unencrypted data in motion presents risks. Such data can also be at risk if it is left in a car that is broken into or stolen on the way from office to home. Moreover, office environments may seem comparatively secure because of systems and personnel in place with responsibility for security, which are lacking in home office environments. We can be sure that criminals will be upping their game to attack soft targets that are out there; we need to be doing the same to stop them. Vocal spoofing presents a vivid example of technology that can be used against us, sending nefarious instructions to personnel masked in the voice of a trusted superior.[24] With communications over the phone instead of in person, can we trust the identity of the person on the line?

The crisis has caused all of us to become more familiar with remote video chats using Zoom and related technology. I have been recording lectures using Panopto, another platform for sharing video recordings and distributing them to students. Numerous others are likely to emerge as the digital marketplace competes for dominance in this new area of consumer and business demand. Although I don't particularly care if others access my lectures or discussions with students, the same is not true of conversations about sensitive client matters. While Zoom is a market leader, recent questions about their privacy practices and concerns about security with people invading and disrupting Zoom conferences present security and privacy concerns that will likely be addressed in the marketplace.

Government investigations by the FTC and privacy regulators elsewhere, including Canada and the EU, will be driving that marketplace toward heightened standards. But what standards will emerge remain unknown. Dynamic conditions and changing standards create a zone of uncertainty for businesses providing and using these technologies but also for the lawyers who must advise on the matter of appropriate security and risk management practices.

Space: A Final Frontier?

Yogi Berra has been credited with the humorous aphorism that "[i]t's tough to make predictions, especially about the future."[25] The above discussion has been light on prediction and focused instead of observable effects arising from technology. But technology and the virtual world ultimately interact with the physical world in which we live and work. How will this interaction affect our need and use of physical space after this crisis ends?

Most of us would have preferred to learn about the benefits of working and meeting remotely on our own terms, but we were "mugged by reality" into learning of them through forced change and adaptation. As my Chinese friend likes to say, "the rice has been cooked." And once that rice is cooked, we cannot put it back into the box. We must eat and enjoy it as best we can. Many of us will value the flexibility, time savings, and productivity benefits of working from a location other than our office. But some may not have developed the physical infrastructure for doing this comfortably.

On the home front, we will probably begin to look for the kind of space that will allow us to work peacefully and effectively. We may need to expand or repurpose space in our living environments to accommodate the new technology we are using. I like my multiple big screens and cannot bear to work from a small laptop. Moreover, I need light to make my camera work effectively. A dedicated home space where I can work with that technology is an essential substitute for my office at work. Here is an area where current tax policy is not friendly to employees. The elimination of the employee business expense with other miscellaneous itemized deductions means that employee expenditures to adapt to the new environment will likely be paid with after-tax dollars. A more tax-efficient approach involves employers bearing those costs. During the current national emergency, special relief may also be available in the form of an exclusion from gross income for employer-provided payments to help employees respond, which may include acquiring technology tools.[26]

Conversely, will these shifts affect our willingness to embrace dedicated office space for all workers? Will the preferences for remote work cause some space to shift to accommodate more group meetings, or at least to accommodate the technology to facilitate group meetings with others who may choose to stay remote from the central office? And are we all going to get big screens and high-definition cameras for our conference rooms, which are now a business necessity rather than another way to watch the Masters in high-definition format when you are working on the weekend during major golf events?

The architects will have to figure this out, but the rest of us will be pondering these questions as we begin to assess the capital we invest in real estate and in technology needed to operate our practices, businesses, and schools. While I will welcome the change that comes when we are all allowed to eat, drink, and meet with our clients, colleagues, and friends—as well as to watch sporting events and films and concerts with them—life will probably not be the same after the crisis ends. We have all changed, too.

Endnotes

1 Tobit 5:3 ("Tobit answered his son Tobiah: "We exchanged signatures on a document written in duplicate; I divided it into two parts, and each of us kept one; his copy I put with the money. Think of it, twenty years have already passed since I deposited that money!") in The Catholic Student Bible 509-10 (Oxford University Press 1995.

2 *See generally* Morse, From Rai Stones to Block Chains, 34 Computer Law & Security Review 946, 950-53 (2018).

3 *See Id.* at 951.

4 *See* Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group, Treas. SM-924 (March 2, 2020).

5 *See* Treasury Sanctions Russia-Based Bank Attempting to Circumvent U.S. Sanctions on Venezuela, Treasury News Release, March 11, 2019.

6 *See, e.g.*, White House Press Briefing by Treasury Secretary Steven Mnuchin on Regulatory Issues Associated With Cryptocurrency, Treas. SM-731 (July 15, 2019).

7 *See, e.g.*, IR-2019-132, July 26, 2019: https://www.irs.gov/newsroom/irs-has-begun-sending-letters-to-virtual-currency-owners-advising-them-to-pay-back-taxes-file-amended-returns-part-of-agencys-larger-efforts

8 *See* Notice 2014-21, 2014-16 I.R.B. 938.

9 *See* Rev. Rul. 2019-24, 2019-44 IRB 1004.

10 Coinbase Help Center, IRS notification, https://help.coinbase.com/en/coinbase/taxes-reports-and-financial-services/taxes/irs-notification.html (accessed April 4, 2020).

11 *See* note 6, *supra*.

12 IRS Operations During COVID-19: Mission-critical functions continue, https://www.irs.gov/newsroom/irs-operations-during-covid-19-mission-critical-functions-continue (accessed April 4, 2020).

13 Nebraska Ethics Advisory Opinion for Lawyers No. 17-03 (September 11, 2017), https://supremecourt.nebraska.gov/sites/default/files/ethics-opinions/Lawyer/17-03.pdf.

14 *Id.*

15 *See id.* (noting conversion will "mitigate the risk of volatility and possible unconscionable overpayment for services).

16 *Id.*

Remember the vulnerability of that half-sheet of paper that Tobit held? *See* note 1, *supra*.

18 Ethics Opinion, *supra* note 13.

19 *See* Neb. R. Prof. Cond. § 3-501.6.

20 Neb. R. Prof. Cond. § 3.501.2(f).

21 *See* Comments to Neb. R. Prof. Cond. § 3-501.6 ("Although the public interest is usually best served by a strict rule requiring lawyers to preserve the confidentiality of information relating to the representation of their clients, the confidentiality rule is subject to limited exceptions. A lawyer may disclose information relating to the representation necessary to prevent a client from committing a crime.")

22 *See, e.g.*, Stephen T. Middlebrook, Sarah Jane Hughes, and Tom Kierner, Developments in the Law Affecting Electronic Payments and Financial Services, 74 Bus. Lawyer 267, 270 (2018-19) (noting concerns from SEC and CFTC chairs about role of lawyers in cryptocurrency transactions).

23 For additional authorities and resources in this area, *see* American Bar Association, Gatekeeper Regulations on Attorneys, https://www.americanbar.org/advocacy/governmental_legislative_work/priorities_policy/independence_of_the_legal_profession/bank_secrecy_act/ (last visited April 4, 2020).

24 *See, e.g.*, Taylor Armerding, Vocal Theft on the horizon, CSO (May 16, 2017), https://www.csoonline.com/article/3196820/vocal-theft-on-the-horizon.html; Larry Johnson, The Latest Thing You Need to Worry About Cybercriminals Hacking? Your Voice, Entrepreneur (August 16, 2018), https://www.entrepreneur.com/article/318238; Jesse Damiani, A Voice Deepfake was Used to Scam a CEO Out of $243,000, Forbes (Sept. 3, 2019), https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/#36a2fbed2241 (reporting actual case of criminal spoofing CEO voice to wire funds).

25 So have others. *See* "it's difficult to make predictions, especially about the future", at https://quoteinvestigator.com/2013/10/20/no-predict/ (suggesting a much older Danish origin for this quotation).

26 *See generally* Richard L. Fox & Joshua D. Headley, Using Employee Relief Funds to Provide Tax-free Assistance, Bloomberg Law (April 2, 2020), https://www.bloomberglaw.com/product/blaw/document/X9BR00QC000000?criteria_id=581e2f3949af9d7bc79a3d6cf72e6439&searchGuid=c6702990-6561-4b04-8bbc-4238abda7080&bna_news_filter=daily-tax-report (subscription required); David Fuller, Disaster Relief Payments – Tax-Efficient Assistance to Employees Impacted by Covid-19, Bloomberg Law (March 27, 2020) https://www.bloomberglaw.com/product/blaw/document/XDI0U9R4000000?criteria_id=581e2f3949af9d7bc79a3d6cf72e6439&searchGuid=c6702990-6561-4b04-8bbc-4238abda7080&bna_news_filter=daily-tax-report (subscription required).