Washington and Lee Law Review

Volume 74 | Issue 1 Article 10

1-1-2017

Appetite for Destruction: Symbolic and Structural Facets of the Right to Destroy Digital Property

Joshua A.T. Fairfield
Washington and Lee University School of Law, fairfieldj@wlu.edu

Appetite for Destruction: Symbolic and Structural Facets of the Right to Destroy Digital Property

Joshua A.T. Fairfield*

Table of Contents

I. Introduction

Daniel Martin has, in his Note *Dispersing the Cloud*,[1] seized on an important and symbolic stick from the traditional property bundle. By showing the vicissitudes the right to destroy has suffered in the transition from Roman to common to modern law,[2] Martin offers us a useful roadmap for the slowly shifting powers we take for granted over what is ours and demonstrates a way forward for one of the oldest of them.

Consumers should have a right to digital destruction for a range of reasons. First, it is a good idea because the power to destroy is highly symbolic. We have long given up Blackstone's

* Professor of Law, Washington and Lee University School of Law.

1. Daniel Martin, Note, *Dispersing the Cloud: Reaffirming the Right to Destroy in a New Era of Digital Property*, 74 WASH. & LEE L. REV. 467 (2017).

2. *See id.* at 8–19 (tracing the history of the right to destroy).

"sole and despotic dominion,"[3] but it is useful to be reminded of the important sense behind that ringing call to battle: that the owner should be permitted to do what she likes with what is hers, insofar as the legal regime can tolerate it. That message is an important one now, when we do not control—and therefore do not own in any recognizable meaning of the term—our smartphones, smart television sets, smart homes, or smart cars.[4]

Second, there is also a deeply practical element to Martin's theory. His argument that digital intangibles *can* be destroyed is, alone, important.[5] The received wisdom is that destruction of digital intangibles is simply too hard, given the nature of information technology and the characteristics of information itself. I will try to show in this brief comment that the naysayers have been too quick off the mark. There are certainly difficulties in securing destruction of information-based property, largely because the transaction costs of copying are so low that computer systems make large numbers of copies purely to function. But the very same systems that are making rivalrous[6] digital property possible make an owner's real power of permanent destruction feasible.

II. Theorizing Destruction

A. Destruction as Guarantor of Property Rules

One core contribution Martin makes to the theory of destruction is to draw attention toward alternative motives for exercising the right to destroy. Courts are skeptical of destruction

---

3. 2 WILLIAM BLACKSTONE, COMMENTARIES *2.

4. *See* JOSHUA A.T. FAIRFIELD, OWNED: PROPERTY, PRIVACY, AND THE NEW DIGITAL SERFDOM (forthcoming 2017) (manuscript at 2) (on file with author) ("We own and control fewer and fewer of the products that we must use to function in modern society.").

5. *See* Martin, *supra* note 1, at 52–55 (addressing the "the question [of] whether cloud-maintained digital property is even capable of deletion").

6. "Rivalry is the inherent characteristic of traditional property that limits control of the property, at any given time, to one person . . . . Intangible rivalrous property, such as an email address, is an example of virtual property. By appropriating an email address for personal use, the user excludes others from using it." Charles Blazer, *The Five Indicia of Virtual Property*, 5 PIERCE L. REV. 137, 143 (2006).

of scarce resources for spite's sake.[7] Perhaps, Martin theorizes, courts might be more open to the destruction of non-scarce (but still rivalrous) resources for the purpose of securing the owner's peace of mind.[8] The question is whether there are other motivations for destruction that might resonate with courts that fall closer to Martin's peace of mind theory on the spectrum than to the spiteful destruction of scarce resources.

The game theoretic thrust of destruction is that it disincentivizes attempts to seize the asset against the will of the owner through some form of liability rule[9] or outright theft. Consider the archetypal game of *chicken*: "Two hooligans with something to prove drive at each other on a narrow road. The first to swerve loses faces among his peers. If neither swerves, however, a terminal fate plagues both."[10] One of the key moves is to rip out the steering wheel—that is, to ensure that if the other party continues on its path, there will be a crash. Technology can serve as the precommitment strategy—the steering wheel remover. This is the standard arrangement on an iPhone: if a potential intruder continues on their course of action of guessing wrong passwords, the phone will automatically delete the encryption key, rendering the data inaccessible.[11] This strongly

---

7. *See, e.g.*, Eyerman v. Mercantile Trust Co., 524 S.W.2d 210, 217 (Mo. Ct. App. 1975) (finding that "senseless destruction serving no apparent good purpose is to be held in disfavor").

8. *See* Martin, *supra* note 1, at 35 (arguing that "peace of mind, certainty, security—however one wishes to phrase it—is a fundamental aspect of property law").

9. *See* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1092 (1972) ("Whenever someone may destroy the initial entitlement if he is willing to pay an objectively determined value for it, an entitlement is protected by a liability rule.").

10. Mikhael Shor, *Game of Chicken*, GAME THEORY.NET, http://www.gametheory.net/Dictionary/Games/GameofChicken.html (last updated Sept. 1, 2006) (last visited Mar. 2, 2017) (on file with the Washington and Lee Law Review).

11. *See* Alina Selyukh & Camila Domonoske, *Apple, The FBI and iPhone Encryption: A Look at What's at Stake*, NPR (Feb. 16, 2016), http://www.npr.org/sections/thetwo-way/2016/02/17/467096705/apple-the-fbi-and-iphone-encryption-a-look-at-whats-at-stake (last visited Mar. 2, 2017) (describing the iPhone's encryption system) (on file with the Washington and Lee Law Review).

disincentivizes theft, as the technological encryption key wipes out valuable data, denying the thief a large part of her gains.

In this sense, then, the power to destroy serves not just to give the user peace of mind that data contained within a destructible digital asset is gone forever, but a more robust peace of mind: the idea that the asset will be destroyed rather than involuntarily transferred, accessed, or used. It strikes me, therefore, that destruction serves as a particularly effective guarantor of property rules against liability rule attempts to seize the asset. Consider the destruction of assets after death. Perhaps the testator believes that the person who is attempting to acquire the property is simply waiting for the testator's death instead of negotiating for the acquisition of the asset. A will with a destruction clause in this context is not born from spite, but social technology, an analog version of the iPhone's digital "dead man's switch." The effect of either is that it is much harder to circumvent negotiating with the owner to access the asset by waiting for her to die (in the case of a will) or trying to hack the phone while out of the owner's possession (in the iPhone's case). The relevant peace of mind is therefore peace from harassment and intrusion for existing assets, as well as the peace that flows from the permanent destruction of past assets. Of course, this does not deal with the court's opposition to the waste of destroying scarce assets, but as the next section discusses, the assets Martin discusses are often rivalrous, but not scarce.

B. Threading the Needle

Martin's theory neatly threads the needle between scarcity and rivalrousness. American courts have consistently disfavored the right to destroy scarce resources, on grounds of waste.[12] If the resources Martin references were truly scarce, then there is every chance that courts would remain hostile to a right to destroy.

Digital resources, however, are often not scarce. For example, it takes only a click of a mouse to generate a million extra copies of the latest pop hit. This raises the other problem, though: intellectual property issues aside, how can anything so easily

12. *See* Martin, *supra* note 1, at 13–15 (discussing cases in which courts limit the right to destroy on the basis of waste).

copyable be destroyed? Both computers as end nodes and computers as connecting nodes of an informational network operate solely on the basis of copying. Both technology and economics drive the massive redundancy of digital resources. Computers convey information by copying, retain copies to verify transmission, backup copies to insure against failure, and, most importantly in the data economy, gather and sell enormous and evolving user datasets as the primary method for monetizing internet services.

To thread the needle, it is useful to note that there are emerging classes of rivalrous, non-scarce assets. This is most clearly seen in the license server model. Consider 1,000 copies of a digital asset, whether a game, an MP3, or a unit of a digital currency. One centralized server can keep a list of who owns what, and if we use the Bitcoin blockchain protocol—which we'll talk about below—we don't even need a centralized server. If my specific digital copy is copy #547, then it does not matter whether it can be duplicated. That copy #547 is linked to a database in the server, and if that particular copy is duplicated, then the server will know that the second linked copy is illegitimate. Similarly, the mechanisms of rivalrousness provide the means of effective destruction. If the license server terminates the entry, then copy #547 is no longer a legitimate copy. That is not total destruction, but combined with encryption and the storage of some resources on the server (so that the client asset, once de-linked, is useless), we can use the emerging technology of digital rivalrousness to effect digital destruction.

Bitcoins are a prime example of this sort of technology. Bitcoins, of course, are intangible, mere entries in a decentralized database called the blockchain.[13] Because these entries on the blockchain are secured by encryption, then only a person with a specific encryption key can access or transfer a Bitcoin.[14] If that encryption key is lost or deleted, the Bitcoin is permanently lost. This is called "burning" in the Bitcoin community,[15] and made for

13. *See* Joshua A.T. Fairfield, *BitProperty*, 88 S. CAL. L. REV. 805, 814 (2015) (describing Bitcoins and the blockchain technology).

14. *See id.* at 820 ("Each person within the property system has a pair of cryptographically related keys, one public, given to everyone in the world to use, and one private, held only by the individual.").

15. *See* Antoine Le Calvez, *How to Destroy Bitcoins*, MEDIUM (Nov. 16,

some of the most compelling early stories. One Bitcoin user threw out the hard drive on which his Bitcoins (or, more accurately, the encryption keys that validated his ability to transfer them) were stored, and the hard drive went to the landfill.[16] He lost $7.5 million worth of Bitcoin as surely as if he had converted them to cash and burned it.[17]

Another example comes from the virtual community *Eve Online*, a massively multiplayer online science fiction game where players can exchange real dollars for virtual objects (and vice versa) and engage in virtual battles that therefore cost real money in terms of virtual objects destroyed. One battle saw the destruction of over $200,000 worth of virtual spaceships and equipment.[18] All questions about why players value video game objects at thousands of dollars aside, the mechanisms of rivalrousness enabled the destruction of those ships. The game provider keeps track of which assets are connected to which accounts. When a ship is destroyed, the data entry is changed, and the player no longer has that ship within the game.

For intellectual property, the problem is the nature of intellectual property itself. Judge Posner noted that the difference between personal and intellectual property is the marginal cost of creation.[19] For personal or real property, the marginal cost of creation does not go down. Manufacturing the nth computer costs about as much as manufacturing the n+1st. But making the first recording of a new song has a vastly

---

2015), https://medium.com/@alcio/how-to-destroy-Bitcoins-255bb6f2142e#.erj44cdsd (last visited Mar. 2, 2017) ("Burning Bitcoins is making them unspendable.") (on file with the Washington and Lee Law Review).

16. Alexander Smith, *IT Worker Throws Out Hard Drive, Loses $7.5 Million Bitcoin Fortune*, NBC NEWS (Nov. 29, 2013, 7:57 AM), www.nbcnews.com/news/other/it-worker-throws-out-hard-drive-loses-7-5-million-f2D11669738 (last visited Mar. 2, 2017) (on file with the Washington and Lee Law Review).

17. *Id.*

18. Rich McCormick, *Spaceships Worth More Than $200,000 Destroyed in Biggest Virtual Space Battle Ever*, VERGE (Jan. 29, 2014), www.theverge.com/2014/1/29/5356498/eve-online-battle-sees-200000-dollars-worth-of-spaceships-destroyed (last visited Mar. 2, 2017) (on file with the Washington and Lee Law Review).

19. *See* Richard A. Posner, *Intellectual Property: The Law and Economics Approach*, 19 J. ECON. PERSPECTIVES 57, 62–64 (2005) (discussing the transaction costs of intellectual property).

different cost than copy-pasting the MP3 once it has been recorded. Of course, manufacturing brings economies of scale, and 3D printing perhaps brings lower marginal costs to physical duplicates without such economies, but the marginal cost of duplicating intellectual property is so close to zero that even the lowest marginal costs of producing personal property cannot come close.

Martin does not differentiate between the categories of emerging rivalrous intangible property and non-rivalrous intellectual property. His cloud examples contain elements of each, with an additional element of personal interest.[20] At several points he makes his strongest argument, which is that at least digital property originating from the self should be subject to the right to destroy.[21] That's clever, and provides a potential bridge between European jurisprudence, where a right to delete is taken seriously, and American jurisprudence, where property intuitions are stronger than privacy intuitions.

So, to what shall we apply this right to destroy? If it is to smart property, the ability to destroy proceeds from the physicality of the linked hardware. If to intangible personal property—not intellectual property—then we must distinguish between intangible property that is rivalrous and intangible property that isn't. That difference is important because we will be able to use the systems set up to make a digital thing unique to be able to destroy it. Non-rivalrous digital property comes close to intellectual property, where we have our greatest difficulties. Here the problem is the raw multiplicity of copies that propagate throughout a system. That, combined with the fact that most information technology systems are almost fiendishly designed to retain duplicates of information, means that the right to destroy could turn into a game of whack-a-mole.

Martin references "the cloud," but just as quickly notes that nobody knows what that is.[22] In the case of digital property, the cloud includes two models that have quite different impacts on

---

20. *See* Martin, *supra* note 1, at 19–29 (discussing digital property managed via cloud storage services).

21. *See id.* at 5–7 (discussing the hypothetical example of a photographer attempting to delete her digital, cloud-maintained photo file).

22. *See id.* at 24 ("What is the cloud? Even among industry experts, the answer to that question is up in the air.").

the theory he proposes. The first is that the cloud might operate on a license server model. This is an attempt to make the digital assets unique by linking them to a register. The second is that the cloud might operate on a backup model. Here, the goal is to enable the computer to recover from nearly any failure by saving and backing up the data as much as possible. Of course, the two can work together, with redundancy serving as the backup to the license server information. But in a legal sense, the two operate quite differently: the license server model lends itself to personal property descriptions. The redundancy model more closely tracks discussions of intellectual property.

Are the differentiations useful? Should we describe a new property form (*pace* Henry Smith and Tom Merrill's *Numerus Clausus*)[23] that somehow captures the emerging consensus around intangible personal property? Or are the concerns about control and finality that Martin describes universal to both intellectual and intangible personal property?

I believe that there is value in distinguishing between intellectual property and intangible personal property, largely because my personal academic project is the recognition of consumer interests in the software, digital assets, and virtual objects that they purchase. The value in continuing to conflate intellectual and intangible personal property is that it would permit users who have some sort of origination right to their data to exercise intellectual property controls, including the right to deny use of that data to anyone else.

C. Privacy, Property, and Origination

This, then, is the core of Martin's argument, as applied to data that originates in an individual. Traditional property rights give a right to destroy. People wish that certain data about them could be destroyed. Some of that data is held in digital objects, like Google Docs, that are the spiritual successors to papers that would have traditionally been deemed personal property. American courts have been liberal in granting citizens property remedies, including the very easy remedy of not doing anything

23. Thomas W. Merrill & Henry E. Smith, *Optimal Standardization in the Law of Property: The Numerus Clausus Principle*, 110 YALE L.J. 1 (2000).

to disturb the owner's decision to delete or destroy. Martin's example of the "Will it Blend?" video series is instructive.[24] No matter how troubled the right to destroy may be in terms of a testator's right to burn down her house after her death, it is quite improbable that destruction of an iPhone would generate any form of legal liability.

There is no question that a right of ultimate disposition—a right to destroy—would help with the project of protecting personal data. The difficulty is that it involves odd contours in the law of property. We have never propertized data. Facts are neither owned as a matter of intellectual property, nor considered personal property. The confusion stems from the fact that some data used to be contained within personal property, and the destruction of the personal property entailed the destruction of the data.

III. Operationalizing Destruction

It is my contention that the difference between raw unowned factual data, intellectual property, and rivalrous intangible personal property has significant explanatory power over our ability to actually destroy cloud-stored intangibles. Intellectual property, like other forms of data, can only be destroyed if encrypted. Intangible personal property (which, somewhat confusingly, can include specific *copies* of copyrighted material) has the additional advantage of being able to leverage the mechanisms of rivalrousness to functionally destroy the digital artifact.

A. Encryption

Even if data itself is not property, the digital boxes that contain it might be. And those boxes can be destroyed. Consider, for example, best practices for data stored with a cloud provider, like DropBox, that may release the information to parties without

24. *See* Martin, *supra* note 1, at 2–3 (discussing an advertising series that literally blends "unconventional items, from toy cars to cans of soup" to, in one feature, an iPhone).

the data originator's consent (in the case of DropBox, most commonly in response to a warrant or administrative subpoena).[25] Users can create encrypted volumes with the cloud provider, making it impossible for the cloud provider to disclose the data. Insofar as the data remains within the encrypted volume, it is subject to destruction. Just as the owner of a Bitcoin can delete the encryption key that permits her to access or transfer Bitcoins, so the owner of an encrypted volume can delete the encryption, irreversibly wiping the contents.

Recall the incident in which the FBI wished to enter one of the San Bernadino shooters' iPhones.[26] The data within the phone was encrypted, and Apple did not have the encryption key.[27] The FBI attempted to pressure Apple into using its software distribution network to accept malware as an over-the-air update, which would disable the encryption function.[28] The point here is that the FBI needed a back door because it could not get through the walls. The risk in that case was that after a limited number of password guesses, the phone would erase itself, or, more precisely, erase the encryption key used to access the phone's contents.[29] Without that tiny bit of information, no known technology can recover the data.

That is destruction of data, complete and irreversible. Of course, the data has to be within an encrypted container, but that is not difficult to manage. In a way, the encrypted container method of destruction works particularly well for the cloud services model. It permits the data to be remotely accessed and stored, and even to be backed up (in encrypted form) by the cloud services provider. Once the key is gone, however, the encrypted data is inaccessible for good, no matter where stored or how many times it has been backed up or copied.

---

25. *See* BRUCE SCHNEIER, DATA AND GOLIATH 67 (2015) (describing how law enforcement agencies such as the FBI obtain information from third parties such as Dropbox).

26. *See* Selyukh & Domonoske, *supra* note 11 (discussing the incident).

27. *Id.*

28. *Id.*

29. *Id.*

B. Leveraging Rivalrousness

The second component of operationalizing a right to destroy will be to use the systems of rivalrousness that currently govern intangible property. This method will of course only work for those systems for which managed rivalrousness matters. The example of an MP3 is instructive. An MP3 may be tracked by a license server, and if it is, then destruction of the link between the MP3 and the license server will have an effect. Consider one older DRM model under which some songs were not playable unless the license server indicated that the user's copy checked out. (Nothing in this Comment promotes such DRM license-server models. I merely note that it is possible to use DRM license-server models to operationalize destruction.) *If* the value of the asset is that it remains linked to the central list of who owns what, then the value of the digital asset can be destroyed by de-linking it from the central list. Another example is a valuable digital asset in a video game. The value of the asset is that it can be used in a shared environment. If I have an awesome hat in *Team Fortress 2*, others can see it and admire my sartorial skills and presumed gaming prowess. The point is that the value of the item is not in the pixel but in the network and social context in which the item appears. It does me no good to have a piece of valuable virtual personal property if there is no one to admire it.

Since the game creator's central server, or the MP3 licensor's license server, dictates who has a legitimate copy of the asset, it is possible to destroy assets by destroying the legitimacy of the link. This is how a game company can destroy a valuable weapon in a game, even though the resource, the code for the sword, still resides on the user's computer. And nobody cares how many times the pixels are drawn, erased, and redrawn. Those are not the essence of the digital property. The essence of the digital property lies in the legitimacy of its appearance within the game. By de-linking the asset, it no longer appears in a game character's inventory. By de-linking a downloaded game, it is no longer available in a buyer's Steam library. By de-linking a book, it is no longer available in the user's Kindle collection. By de-linking an iTunes song, it is no longer available in the iTunes library. And so on.

The key here is that the legitimacy of the asset is destructible. With legitimacy comes convenience. It very convenient to download an asset once one has legally purchased it. Illegally obtaining and accessing software, music, or even hacked versions of networked assets like equipment within a game is costlier in terms of time and effort. Note that I do not claim it is impossible to obtain illegitimate copies, or even particularly difficult. But small transaction costs have large effects on low-value, high-volume transactions. Buying a Kindle is simply easier than trying to download a million ebooks from the Pirate Bay.

IV. Conclusion

Martin's take on destruction divorces the debate from the American-frontier focus on preserving scarce resources against waste. It also creates a fascinating space between rivalrousness and scarcity, in which courts may be willing to enforce a right to destroy where there is no waste, and those rights are practically enforceable because the technological systems that undergird digital rivalrousness. For instance, destroying the data on an iPhone or a blockchain entry might be supported by courts because it is not waste, and is enforceable as a practical matter because of container encryption and distributed ledger technology.

The practical effects of a strengthened theory of destruction also lead to a deepening of Martin's theory of peace of mind. Peace of mind in the more constrained sense relates to being sure that data, once deleted, is gone. That's a hard row to hoe, given the redundancy of information processing systems. A deeper peace of mind might relate less to the final and total deletion of information and more to the incentives potential expropriators might have to circumvent negotiation with the owner.