Annual ADFSL Conference on Digital Forensics, Security and Law

2017
Proceedings

May 16th, 9:15 AM

Defining a Cyber Jurisprudence

Peter R. Stephenson PhD
independent researcher in cyber jurisprudence, pstephen@cdfs.us

DEFINING A CYBER JURISPRUDENCE

Towards Evolving the Philosophy and Theory of Cyber Law: A Foundational Treatise

Peter R. Stephenson
Leicester University Law School
Leicester, UK
prs33@leicester.ac.uk

ABSTRACT

Jurisprudence is the science and philosophy or theory of the law. Cyber law is a very new concept and has had, compared with other, older, branches of the law, little structured study. However, we have entered the cyber age and the law - on all fronts - is struggling to keep pace with technological advances in cyberspace. This research explores a possible theory and philosophy of cyber law, and, indeed, whether it is feasible to develop and interpret a body of law that addresses current and emerging challenges in cyber space.

While there is an expanding discussion of the nature of cyber law and its challenges, a significant body of scholarly contributions to the discussion is lacking. Focus, in the main, is on the practical aspects of cybercrime rather than the theory, philosophy and science of cyber law generally. We seek to define, as a contribution to the discussion, the jurisprudential aspects of thinking about cyber law. Specifically, we seek to develop a broad measuring stick that can be applied to cybercrime as well as to legal constructs outside of cybercrime (tort, contract, international, etc.). This paper sets the foundational starting point for the research in progress by establishing a context for cyber jurisprudence.

Keywords: cyber, crime, tort, jurisprudence, law, cyber law, cybercrime, cyber science

1. INTRODUCTION

No discussion of cyber law can begin effectively without defining a baseline of terms. Cyber law itself is not well-defined and, in fact, it is conceivable that, from a practical perspective, there is no such thing.

For example, Murray in his paper "The Law of the Horse" is quite clear that we should reason from the general to the specific and that we learn more about the specific by understanding the general case. (Murray, 2013) Murray recalls a talk in which the question arose as to whether there needs to be a law of horses. He notes that there are laws relating to horse racing, veterinary care of horses, laws relating to being kicked by a horse, and quite a few others. "Should there be," he asks "a general law of the horse to cover all of these situations under a single heading?" His conclusion is that there should not be such a law.

That in mind, then, do we really need "cyber law?" Is defining a body of cyber law simply a twenty-first century "law of the horse?" The contention of this paper is that there should, in fact, be a coherent body of cyber law as well as

guidelines for applying traditional law (from the physical world) in cyber situations.

The thesis statement for this research is:

> It is feasible and necessary to create an extensible jurisprudential approach to law that admits of and keeps pace with cyber science without being a set of restrictive guidelines that are both confining and resistant to change.

This paper addresses the foundational elements of the research project as a whole, setting a baseline from which to work and beginning the process of answering the thesis question.

To address the topic of cyber law it is helpful to undertand exactly what we mean by such terms as cyber law, cyber science, cyber crime and cyber jurisprudence. That is where this paper begins in Section II.

Section III sets the stage for further discussion by presenting a brief discussion of the theory and philosophy – the jurisprudence – of the law. We take up a few different areas of the law and the thinking behind them.

In Section IV, we apply the definitions in Section II to the framework in Section III to establish where – if at all – cyber law fits into "The Law."

In Section V, we draw conclusions about cyber law and its place in the legal system as it emerges into the twenty-first century. And in the final section – Section VI – we propose areas for further research and discussion.

I. Definitions

1.1 Cyber Science

Ma, Choo, Hsu, et al have a definition of cyber science that we can use as a starting point (Ma, et al., 2016):

> *Cyber science is concerned with the study of phenomena caused or generated by the cyberworld and cyber-physical, cyber-social and cyber-mental worlds, as well as the complex intertwined integration of cyber physical, social and mental worlds.*

Because the strong implication is that cyber science is related to some sort of interaction within the cyber space and the physical space, our working definition takes these interactions into account:

DEFINITION 1 – Cyber Science

> Cyber science is the study of phenomena caused or generated within the cyber space, which may or may not interact with phenomena caused or generated within the physical space.

Note that it is a requirement of the definition that the phenomena be *caused* or *generated within* the cyber space. This preculdes phenomena that are generated within the physical space and, for one reason or other simply touch the cyber space. To clarify this relationship, it is useful to define concisely the roles that a computing device may play in such an interaction.

Computing devices can play one or more of three roles: (1) the source of a cyber event, (2) the target of a cyber event, and (3) the repository of evidence relating to a cyber event. So, for example, the theft of a computer containing the evidence of a crime, while, perhaps, fitting the criterion number (3), is not an example of the application of cyber science because the action is entirely within the physical space. However, the theft of passwords from the same computer may be because accessing the computer, removing the password file and cracking the passwords in the file likely is a cyber event in toto.

1.2 Cyber Law

There are several rather lengthy and not particularly useful definitions of cyber law. In

the absence of a concise statement of what cyber law is and what it comprises there appears to be a tendency to view everything that touches the cyber space – no matter how obliquely – as worthy of cyber law.

In other words, we are getting dangerously close to Murray's Law of the Horse (Murray, 2013) wherein he recalls that there are lots of laws that have something to do with horses so why not bundle them all together into a "law of the horse." Obviously, this is neither necessary nor is it a useful approach since some of the laws – most, probably – that might be interpretted as having something to do with horses also are torts.

The Cyber Laws web site gives us a moderately useful definition of cyber law (Laws.com, 2017):

> *Cyber laws can be defined as legislation, legality, and practice of lawful, just, and ethical protocol involving the internet, as well as alternate networking and informational technologies.*

However, even this definition lacks precision. Parsing the definition, applying cyber science, and looking to the philosophy of law – which tells us that law is defined broadly as obligation – we get an opportunity to apply logic:

S1. Law is broadly defined as obligation and duty (Green, 2002);

S2. Cyber science applies to the study of phenomena caused or generated within the cyber space;

S3. Cyber law should apply specifically to law as related to cyber science;

S4. Therefore, cyber law should be defined in terms of cyber science and the obligations and duties created by the Law.

DEFINITION 2 – Cyber Law

> Cyber law is the set of obligations and duties applied to events related directly to cyber science.

Everything that falls outside of this definition is traditional law. Cyber law deals exclusively with legal issues in cyber science. That is not to say that we need a set of new laws that apply to everything that could occur in the cyber space. In fact, even traditional laws may be interpreted in the context of cyber law if appropriate. In these cases, the occurance of a cyber event – as described within the constraints of cyber science – simply needs some common sense adjustment to accommodate the cyber space. However, events that occur uniquely in cyber space – and are subsumed in cyber science – likely will need their own laws.

1.3 Cyber Crime

While it may seem obvious that cyber crime is any act that violates a cyber law, what about acts that violate traditional laws but take place exclusively in cyber space? For example, let us suppose that victim V is being stalked on-line by defendant D. Do we need a special law for cyber stalking or can we apply a generic stalking law and interpret it in the context of on-line activity?

Researchers have proposed that there are specific and significant differences between physical stalking and cyber stalking (Bocij, 2004). Bocij's definition of cyber stalking (p. 14), however, simply renames traditional stalking media and acts as cyber stalking media and acts. With this in mind courts, arguably, have all of the tools needed to try a cyber stalker without resorting to a new law just for cyber stalking. Lousiana stalking law is typical of those laws found throughout the United States (Lousiana Legislature, 2017):

> *Stalking is the intentional and repeated following or harassing of another person that would cause a reasonable person to*

> *feel alarmed or to suffer emotional distress.*

One easily could apply this law to both physical and cyber stalking. In fact, research suggests that the two often occur together (Stephenson & Walter, 2011). There are multiple types of acts that we may consider when we consider cyber crime. Not all fit the definition of "crime."

For example, some may be private law such as torts. The Justia legal dictionary defines a crime as (Justia.com, 2017):

> *Something you do, or don't do, that breaks a law that says you can't do it or must do it.*

Dripps, Boyce, and Perkins, in Criminal Law and Procedure – 12th Edition, (Dripps, Boyce, & Perkins, 2013) quote the eminent 18th century jurist and legal scholar Blackstone's definition of crime:

> *A crime or misdemeanour is an act committed or omitted, in violation of public law either forbidding or commanding it.*

Torts are defined by Dobbs (Dobbs, 2000) as:

> *Conduct that amounts to a legal wrong and that causes harm for which courts will impose civil liability.*

So, obviously, we need a definition of cyber crime that is broader than the strict definition of "crime." However, the definition of crime may be seen to subsume, at some level, civil law. In fact, it is not uncommon for a plaintiff to seek redress at civil court for a wrong that has been tried in criminal court. In such cases evidence developed in the criminal action is usable in the civil proceeding.

There are major differences, however. Crimes are wrongs against society in general which demand punishment while torts are wrongs against individuals which demand redress. Skwirk.com, an online education resource, differentiates between crimes and civil laws such as torts (Skwirk.com, 2017):

> *Criminal law involves a relationship between the Crown (State) and an individual. Civil law, on the other hand, involves resolving all other disputes.*

It is important to differentiate between torts and crimes in the cyber space just as it is in the physical space. Although, as we will see, there are only a few – but a very important few – differences between tort law and criminal law. Therefore, just as in the physical space we need to acknowledge those differences and account for them in our deliberations.

DEFINITION 3 – Cyber Crime

> A cyber crime is crime or misdemeanour ocurring in the space defined by cyber science and comprising an act committed or omitted, in violation of public law either forbidding or commanding it.

DEFINITION 4 – Cyber Tort

> A cyber tort is a breach of duties fixed and imposed upon the parties by the law itself in the space defined by cyber science without regard to their consent to assume them, or their efforts to evade them that causes harm and for which courts will impose civil liability.

The reader will, perhaps, note that these definitions stick very closely to the traditional definitions of crimes and torts in the physical space. That similarity is intentional because, as one will see in Section V following, establishing the cyber context of crimes and torts follows very closely the approach to the establishing of context for crimes and torts in the physical space.

1.4 Cyber Jurisprudence

To define cyber jurisprudence, we must define jurisprudence first. In the context of this research, Black's Law Dictionary gives us two useful definitions of jurisprudence (Garner, 2010).

> *A method of legal study that concentrates on the logical structure of law, the meanings and uses of its concepts, and the formal terms and modes of its operation.*

and

> *A system, body or division of law.*

Both of these definitions are useful because they cover the general – sometimes stated as the theory and philsophy of law – and the specific – a system or body of law. The first definition from Black's gives us the approach to this research, results of which which we intend to lead to the second definition.

DEFINITION 5 – Cyber Jurisprudence

> Cyber jurisprudence is the legal study that concentrates on the logical structure, the meanings and uses of its concepts, and the formal terms and modes of operation of cyber law.

II. Jurisprudence Generally

We can apply the notion of jurisprudence to all facits of the law, allowing us to reason about them in a relatively structured manner. For our purposes – and as a brief introduction – here we address criminal law and the law of torts. We address these aspects in the current section in general. We will apply the theory – again, briefly as an introduction – to cyber law in Section IV. We select criminal and tort law here because they offer contrapuntal views of the interaction and consequences of an actor's negative acts with the actor's victim.

1.5 The Jurisprudence of Criminal Law

There are many ways to approach the philosophy of criminal law. Alexander (Alexander, 2002) choses to approach it through justifiable legal punishment. He defines this approach as,

> *One is justifiably punished if one deserves punishment, and one deserves punishment in virtue of acting (or, in some cases, failing to act) with insufficient concern for the interests of others for which one is obligated to act with concern.*

This is consistent with the notion that criminal law treats those offenses that are against the public good and for which the state exacts a penalty. Legal theorists approach punishment as retribution, consequential or threat-based. Retributivists see punishment as a sort of "eye-for-an-eye" approach. Consequentialists see punishment as the consequence produced by some act. Threat-based theorists believe that threatened punishment, if severe enough, will have a preventative outcome. Two of these theories are at play most dramatically in our legal system when we compare punishment of adults – retributive, and children – threat-based.

There are some basic premises attached to the system of criminal law in the United States. First, a law cannot be retroactive. In other words, a crime committed before it was defined as a crime cannot be addressed at a later date if the act should at some future time become illegal.

Second, the criminal act must be voluntary (Dressler, 1995). Criminal culpability can be purpose, knowledge or recklessness. Culpability also can be based upon negligence or strict liability.

Purpose is the mental state of intending to commit an act. For example, when an actor visits a child pornography web site that is one of twenty such sites that he has bookmarked, he is acting with purpose.

Knowledge is when the actor knew – or should have known – that the act she is about to perform is illegal. Recklessness is quite a bit more complicated in that it is subjective and may depend upon the circumstances.

For example, many years ago, when the author's eldest son was a football player in high school the car he was driving was hit broadside by a driver who ran a red light in his hurry to get to a video store before it closed. The consequence was that the author's son suffered a broken collar bone and never was able to play football again. The other driver's action was reckless in that he should have been aware that speeding through a red light for whatever reason was risky business.

Negligence and strict liability are beyond the scope of this discussion and pose some complicated questions that may or may not relate to cybercrime. We'll address one additional issue in the theory of criminal law: uncompleted attempts. In order to be liable for a criminal act the actor must complete an attempt to do the act. Simply thinking about or planning a crime – even if purpose and knowledge are present – is not sufficient to complete the act. This will become important when discussing cybercrime.

1.6 The Jurisprudence of Tort Law

Ripstein (Ripstein, 2002) characterizes tort law as:

> *How should people treat each other? and whose problem is it when things go wrong?*

Tort law, then, differs from criminal law in that it involves wrongs to individuals rather than wrongs against society. Generally, torts fall into the categories of intentional and negligent offenses against an individual, the plaintiff. Those offenses can be against the person, chattels or real property of the plaintiff.

Taking negligence there are some issues that must be addressed. First, is the foreseeability of the consequences of the defendant's act against the plaintiff. For example, if D sticks her foot out in the aisle of a theater and P trips, falls and is injured, it was reasonably foreseeable that D's action could cause injury to some victim.

The second issue is the objective view. In analyzing a tort, we are not concerned with what the defendant thought subjectively; rather, we are concerned with how an objective third party would interpret the act. Generally, the court plays the role of the objective third party.

Keeton, in Prosser and Keeton on the Law of Torts (Keeton, 1984), one of the leading law school texts on the topic, defines a tort as

> *… a breach of duties fixed and imposed upon the parties by the law itself, without regard to their consent to assume them, or their efforts to evade them.*

While a discussion of tort law could consume the bulk of this paper, for our purposes most of it would be out of scope.

III. Applying Jurisprudence to Cyber Law

In order to apply the fundamental notions of criminal and tort jurisprudence to cyber law, we must return to our Definition 2:

> Cyber law is the set of obligations and duties applied to events related directly to cyber science.

We recognize that, applying these notions we have three possible outcomes: (1) there is no relationship between jurisprudence in general and cyber law in particular, (2) such a relationship exists but it does not require a new jurisprudence to understand it, and (3) a new jurisprudence and a new view of cyber law is necessary.

In the first instance we return ot "The Law of the Horse." Everything that we have at present is sufficient and determining outcomes with a special view to cyber science is unnecessary.

Thus we find that no special philosophy or theory of law is necessary to treat events that take place in or touch the cyberspace.

In the second instance we recognize that cyber law is a special area of the law but we acknowledge that current jurisprudential thinking is adaquate to apply existing theory to its study and analysis.

In the third instance we conclude that cyber law is a special and unique field of the law, little existing law or theory is adaquate to address it and it requires its own special and unique philosophical and theoretical treatment.

1.7 Applying the Jurisprudence of Criminal Law to Cyber Law

We begin with the premise of punishment or, as Alexander puts it "deserts" (Alexander, 2002). Does an actor who performs an act in or touching the cyber space that violates an existing law derserve punishment in the same manner as an actor who performs an act that violates an existing law in the physical space? Second, we ask what form those deserts should take. Should they be retributive, consquential or threat-based?

The theory of criminal law is rather straightforward, at least as it addresses part of the question.

> *One is justifiably punished if one deserves punishment, and one deserves punishment in virtue of acting (or, in some cases, failing to act) with insufficient concern for the interests of others for which one is obligated to act with concern.*

So the implication is that any act whether in cyber or physical space that meets these criteria should result in punishment. There is no distinction between application of the criteria. A law has been broken, the actor should have her desserts.

There is nothing in criminal jurisprudence that demands special treatment for acts that occur in the cyber space. Perhaps that is the root of the issue. Are laws that apply in the physical space equally applicable in the cyber space? And, conversly, are there issues that are unique to the cyber space that cannot be addressed by existing laws in the physical space?

The question, then, is not quite as fundamental as it would appear at first blush. Certainly, the notions proffered in Alexander's definition – as far as they go – apply no matter what the venue of the offence is. But is that enough?

Are acts that meet our definition of cybercrime unique enough to require a special theory and philosophy of the law, exclusive to those acts? Or, as we proposed above in our discussion of cyber stalking, are the criteria for a particular offence satisfatory. Addressing the middle road, perhaps the answer to both questions is "yes."

At the core of the issues of criminal law applied in a cyber context might be whether or not an act in cyber space could be an act against society. Certainly when large numbers of individuals, and their basic freedoms, are the target, such as a massive payment card or password breach that puts hundreds of thousands of people at risk, one could make a case for the act being a crime. But is it a cyber crime requiring special teatment?

We have entered an era where cyber attacks could cause everything from inconvenience to death. Certainly that universe of possibilities demands consideration as criminal acts.

1.8 Applying the Jurisprudence of Tort Law to Cyber Law

Since tort law addresses wrongs to individuals instead of wrongs against society it is necessarily somewhat more complicated. However, arguably, tort law from a jurisprudential perspective seems not quite so complicated as it does from the legal practice perspective.

When the author was beginning first year law in a JD program, a law professor colleague gave as a gift a copy of Prosser and Keeton on Torts. In his dedication on the inner cover he quoted a line from author and lawyer Scott Turow in 1L: *Torts is the course that proves your mother was right*. This is an excellent way to characterize tort law. Tort law is about the way we treat each other and what the consequences of bad behavior in that regard are.

Given that and our definition above, the question that remains is- can we treat each other badly in cyber space and if we do are we talking about the same or different maltreatment as we might encounter in the physical space? Of course, if there is no distinction we do not need a separate way of treating misbehavior in the cyber space from the way we treat others in the physical space.

However, we know that every act has consequences. The jurisprudence of tort law has defined the acts with which we should concern ourselves and over time we have evolved a framework of those acts and, generally, the consequences of bad behavior. The framework is called the Common Law and over time it has been refined and restated at least three times in US law. Do we need a new restatement that takes cyber law into account? Perhaps.

The Concise Restatement of Torts Third Edition (Bublick, 2013) brings into focus liability for physical and emotional harm. At the end of Chapter 1 the Restatment explains,

> *Restatements are not simply a "restatement" of what courts have done. In many cases they attempt to synthesize decisions that seem disparate or confused.*

This could be the perfect description of where cyber law fits within the framework of tort law: decisions seem disparate or confused. However, if that is the case what do we do about our original choices as applied to tort law:

> (1) … there is no relationship between jurisprudence in general and cyber law in particular, (2) such a relationship exists but it does not require a new jurisprudence to understand it, and (3) a new jurisprudence and a new view of cyber law is necessary.

Given our definition of tort law, it certainly seems likely that there is an application of some sort for a theory of cyber law as it applies to torts.

IV. Conclusions

While we have examined only criminal and tort law – and neither of those in depth – we can begin to draw some conclusions. These conclusions may help us to frame the answer to our initial thesis question:

> Is it feasible and necessary to create an extensible jurisprudential approach to law that admits of and keeps pace with cyber science without being a set of restrictive guidelines that are both confining and resistant to change?

We will apply, however loosely, the scientific method to our analysis as our approach to drawing conclusions.

1.9 Applied to the Criminal Law

> **Premise 1** - there is no relationship between criminal jurisprudence in general and cyber law in particular.

S1. One is justifiably punished if one deserves punishment, and one deserves punishment in virtue of acting (or, in some cases, failing to act) with insufficient concern for the interests of others for which one is obligated to act with concern (from definition III(A)).

S2. Certain acts in the cyber space constitute such behavior.

S3. Actors perpetrating such acts deserve punishment.

S4. Therefore, there is a relationship between criminal jurisprudence in general and cyber law in particular.

Premise 2 - there is a relationship between criminal jurisprudence in general and cyber law in particular, but it does not require a new jurisprudence to understand it.

S1. There is a relationship between criminal jurisprudence in general and cyber law in particular (from Premise 1).
S2. Certain acts are within the realm of cyber science but are sufficiently like similar acts in the physical space that they may be interpreted similarly.
S3. Certain acts while within the realm of cyber science also are within the realm of physical science and may be interpreted in terms of current criminal law.
S4. There is no need to develop a new jurisprudence for cybercrime.

Premise 3 - there is a relationship between criminal jurisprudence in general and cyber law in particular, and it does require a new jurisprudence to understand it.

S1. There is a relationship between criminal jurisprudence in general and cyber law in particular. (from Premise 1).
S2. Certain acts while within the realm of cyber science also are within the realm of physical science and may be interpreted in terms of current criminal law.
S3. Certain acts are within the realm of cyber science but are sufficiently like similar acts in the physical space that they may be interpreted in terms of current criminal law. (from Premise 2)
S4. Certain acts are uniquely within the realm of cyber science and only may be interpreted in context with cyber science without reasonable recourse to existing criminal law.
S5. Certain acts are in the realm of physical space but are controlled by cyber science and only may be interpreted in context with cyber science without reasonable recourse to existing criminal law.
S6. S4 and S5 preclude Premise 1 and Premise 2 from being valid.

Given that our conclusion is Premise 3, where does that leave us with regards to a cyber jusiprudence of cyber crime? Clearly we are faced with three types of crimes:

(1) Those that are in the physical space only and are not governed in any way by cyber science.

(2) Those that are in the cyber space only and are uniquely governed by cyber science.

(3) Those that co-exist in the physical and the cyber space (call them "hybrid crimes") and are at least in part governed by cyber science.

There is the strong implecation that types 1 and 2 argue for a jurisprudence of cyber crime. However, it appears that such a jurisprudence would not necessarily require rewriting the entire pantheon of current criminal laws. By building on the Model Penal Code (Wechsler, 1962), we may investigate correlations with

existing criminal law and add that which is necessary, either for creating new law, interpretting existing law, or adding to existing law to extend the law into the cyber space where necessary.

1.10 Applied to the Law of Torts

> **Premise 1** - there is no relationship between the jurisprudence of torts in general and cyber law in particular.

S1. A tort is a breach of duties fixed and imposed upon the parties by the law itself, without regard to their consent to assume them, or their efforts to evade them (from definition III(B)).

S2. Certain acts in the cyber space constitute such behavior.

S3. Actors perpetrating such acts deserve to be held liable for their acts.

S4. Therefore, there is a relationship between the jurisprudence of torts in general and cyber law in particular.

> **Premise 2** - there is a relationship between the jurisprudence of torts in general and cyber law in particular, but it does not require a new jurisprudence to understand it.

S1. There is a relationship between the jurisprudence of torts in general and cyber law in particular (from Premise 1).
S2. Certain acts are within the realm of cyber science but are sufficiently like similar acts in the physical space that they may be interpreted similarly.
S3. Certain acts while within the realm of cyber science also are within the realm of physical science and may be interpreted in terms of current tort law.
S4. There is no need to develop a new jurisprudence for cyber torts.

> **Premise 3** - there is a relationship between the jurisprudence of torts in general and cyber law in particular, and it does require a new jurisprudence to understand it.

S1. There is a relationship between the jurisprudence of torts in general and cyber law in particular (from Premise 1).
S2. Certain acts while within the realm of cyber science also are within the realm of physical science and may be interpreted in terms of current tort law.
S3. Certain acts are within the realm of cyber science but are sufficiently like similar acts in the physical space that they may be interpreted in terms of current tort law. (from Premise 2).
S4. Certain acts are uniquely within the realm of cyber science and only may be interpreted in context with cyber science without reasonable recourse to existing tort law.
S5. Certain acts are in the realm of physical space but are controlled by cyber science and only may be interpreted in context with cyber science without reasonable recourse to existing tort law.
S6. S4 and S5 preclude Premise 1 and Premise 2 from being valid.

1.11 Analysis and Possible Solution

As is clear, there are more than passing similarities between the logical proofs of criminal law and tort law above. This is no accident since, as we have seen, the big difference between the criminal law and the law of torts is the univese of those wronged. In the case of criminal law, it is deemed to be society that is the victim while in the law of torts it is the individual. Therefore, with some

mechanical differences we may, for our purposes, treat the two areas of the law similarly.

The conclusion is that there is a need for a jurisprudence of cyber law but that jurisprudence does not dictate a complete new body of laws.

Within the law of torts, as well as several other branches of the law, this need for a synthesis of decisions that seem disparate or confused suggests that some sort of updating of the law of torts and of criminal law. Fortunately, we have a mechanism for doing exactly that.

Within the law of torts, we have the Restatements that allow us to clarify and build upon existing law. Perhaps it is time for a Restatement 4d, or similar.

In criminal law, we have The Model Penal Code. Without materially changing the MPC, we can defer to other books that have sought to build upon and clarify the criminal law such as Dubber's Criminal Law Model Penal Code (Dubber, 2002). Within these scholarly works, we can begin the process of updating the criminal law to address cyber realities of the immediate present and the future.

V. For Further Work

The obvious areas of further research include extending the premises discussed in this paper to other areas of the law such as property law and international law, and devloping guidelines appropriate to the area of law under consideration.

This research is necessarily a work in progress because the law is a work in progress. That suggests that future work deriving from this research should proceed by increasing both breadth and depth of research and application to the law.

