The third edition of Professor Ralph D. Clifford’s \textit{Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime},\textsuperscript{2} guides readers through the U.S. legal process currently in place to address cybercrime. The book has four main chapters each written by a cyber law expert for a particular area. After beginning with a comprehensive overview of federal and state cybercrime laws, readers then get an insider’s view of cybercrime prosecution and defense methods and strategies. Clifford ensures special emphasis is placed on investigatory practices and procedures throughout the book. \textit{Cybercrime’s} concluding chapter focuses on efforts to address cybercrime on an international scale and provides insight into future challenges.

\textit{Cybercrime} is a fantastic resource for law enforcement, attorneys, law students, and anyone interested in learning more about computer crime law. The proceeding section contains an interview with Professor Clifford who shares information on his book and also an experienced perspective on the current state of cybercrime law.

\textsuperscript{1} Ralph D. Clifford is a professor of law at the University of Massachusetts School of Law and is a member of the bars of Massachusetts, New York, and Connecticut.

JHTL: First and foremost, I want to thank you very much for your time both personally and also on behalf of the Journal of High Technology Law for Suffolk University. It’s a great addition to be able to speak with you and hear your thoughts. How did you get into cyber law and what is your background in cyber law?

RC: I started as a computer science person, both with a computer science degree and about 10 years worth of professional programming experience, and then went to law school. So I went into law school with a fair amount of computer science background to begin with and it was sort of a natural thing to put the two together. I've been practicing or teaching computer law, cyber law since about 1984-85. I was in practice in Connecticut for about 10 years at a predominantly business litigation boutique but it also had what then was developing as a computer law practice that mostly involved working with start-up companies.

JHTL: I really enjoyed reading your book and particularly liked the format where you introduced the laws and then provided the prosecution and also the defense sides back to back. How do you come up with the format and how did you select the authors for the different chapters?

RC: I did a continuing legal education seminar, a couple years before the first edition came out, probably 1999 maybe 2000, somewhere in that zone. I put together a seminar on cybercrime and I wanted it to be a little less directed than a lot of CLE stuff is. I'm a firm believer that you cannot be a good attorney if you don't know what the other side is doing and as a consequence I wanted to make sure to cover both the persecution and the defense of cybercrime. Also, since
the investigation issue is so key to the area, I wanted to make sure that the investigation areas were covered very well.

The primary authors, the first three authors were all presenters at my conference. Professor Brennan from University of Dayton is one of the experts on cybercrime in the country. She's one of the first to do it and to do it comprehensively and that's how I chose her. I don't remember how I got Ivan Orton’s name originally. He's been prosecuting cybercrimes – he’s in the Seattle area. Our defense attorney [Joseph Savage Jr.], he's out of Boston and he's done a lot of defense in the area. Then the final chapter, Miriam [Weismann] was not one of the original presenters. She's now at the Suffolk business school as a matter fact, but for awhile she also taught at my law school. So the book then developed out of that conference - I recognized that I had all of these great people on a single e-mail list. I also had contacts with the publisher who had expressed interest to me about a book about cybercrime so I just put the two things together.

JHTL: Having been in print for almost 11 years now, how have you seen cybercrime law change over the course of three editions of your book?

RC: I think the legal response now is more comprehensive than it was when that first edition came out. When the first edition was prepared, a lot - particularly a lot of the academic framework for thinking about cybercrime hadn't been defined and people were not even agreeing what cybercrime was and how to come across with the definition. I think in the interim, that has settled down a good deal and most of the major ways that cybercrimes are committed have now been ensconced in both federal and state legislation. Note I did not say international. With that, federal and state legislation have fairly comprehensively covered the various areas where crime
is occurring. It doesn't mean that there aren’t holes but you know there are some statues that are addressing most of the major ways that people are misusing computer technology.

JHTL: One of the quotes that really struck me in reading your book came from Ulrich Sieber of the Max Planck Institute for Foreign and International Criminal Law. Specifically he said: “The Internet is fast whereas criminal law systems are slow and formal. The Internet offers anonymity whereas criminal law systems require identification of perpetrators. The Internet is global whereas criminal law systems are generally limited to a specific territory… Effective prosecution with national remedies is all but impossible in a global space.”3 Do you agree with the sentiment of his last sentence that prosecution on a global level is all but impossible?

RC: Not really - and I think the example I would cite right now is the MegaUpload indictment - that was clearly one of the international criminal enterprises, assuming at this point everything in the indictment is true. So, if the accusations are true, though that was clearly an internationally based criminal conspiracy it will never the less be prosecuted within the nation’s boundaries. There's been a fairly long history if you think about it of imposing criminal charges on conduct that has not occurred within the nation’s boundaries. You can't always get the individual in your court system but that doesn't mean that the indictment can't be brought, that a criminal prosecution can't be triggered. So I don't think his final statement is completely true because there can be effective prosecution. There are areas where it is extremely difficult, much more so to do with getting information than anything else - than necessarily having to have some kind of international remedy.

3 Clifford, supra note 2, at 257.
JHTL: So do you think that things like the Council of Europe and its Cybercrime Convention aren't really necessary for international prosecution?

RC: I think that the strongest parts of the Cybercrime Convention are not the parts that are trying to define cybercrime for us but the parts that are trying to establish mechanisms of enforcement, mechanisms of information acquisition. So I think that there's a very, very important role for international treaties and laws but I think their more important role is always going to be providing access to information from overseas rather than some type of international tribunal if you will. I don't ever see a cybercrimes tribunal like we now have a war crimes tribunal. That would be very surprising.

JHTL: How do we get other nations on the same page and in agreement for the things you just spoke about?

RC: I'm not sure you ever can. In the same ways that even the relationship between U.S. states gets to be very clumsy, when you move internationally different people have different morays, different ways of running their system and there’s never going to be enough unanimity about how that's done to make an international treaty an easy thing. You can just compare the best areas to consider - what the United States considers freedom of speech and what most of the world considers freedom of speech. There are amazing differences in the way that speech is sometimes criminalized overseas and even regulated. Even if you look at the British pattern,
they don't have a *New York Times v. Sullivan*[^4] type role for the First Amendment. It doesn't matter if you're a public figure, if you libel them or slander them; so even two very close allies and close democracies like the United States and England have two very different rules. How are we going to ever possibly get the United States and Iran or the United States and Venezuela, to come up with rules that both will accept? I don't know - I don’t think that's practical.

**JHTL:** How do you feel about the current state of U.S. cyber law in terms of its adequacy in addressing cybercrime?

**RC:** As I [previously] indicated, the most important areas have a check mark in them now. Whereas if you look back 20 or 30 years ago, there were major things going on that were clearly criminal-like in nature but were not thought of as crimes and I think most of those major areas have been covered now. I think the biggest problem, and this is particularly true at the federal level, is that a lot of the ways that our cybercrime statutes work are based on a model of computerization that no longer exists. In fact, have you ever seen the movie *War Games*? It's sort of a stupid little move but the point of it is that a lot of our cybercrime legislation – [15 U.S.C. §] 1030 being a classic example, has in its picture and its target, this idea of somebody sitting there and dialing into somebody else's computer to gain access. And as a practical matter, that's not the way it happens anymore because all of these computers are now Internet-connected. And that makes the analysis of whether or not the access was authorized or unauthorized much more complicated than it used to be. And that's not something that 1030 addresses well.

Is it unauthorized access for me to get on my employer’s computer and do something that I'm not supposed to do or if you get onto a university system and you do something buried away

in some policy somewhere where it says you’re not supposed to do? It becomes a very difficult analysis when the normal mode on the internet and the web is open. How do we know when the door has been shut? I don't think 1030 addresses that well at all or many of the other provisions that address the improper access to a computer system.

JHTL: Well that couldn't have been a better lead in to my next question. I'm doing my note as a further examination of contract-based interpretations of what constitutes authorized access. I'm sure you're familiar with the recent opinion by the 9th Circuit in *Nosal*, and how they granted an en banc rehearing of that case, which happened in December. What is your view of establishing a contract-based interpretation of what constitutes authorized access under the Computer Fraud and Abuse Act?

RC: I think it's an area that's absolutely fraught with all kinds of policy problems. In general, I don't see how you can talk about unauthorized access without looking at the contract between the parties, whether a legal contractor an implied contract - implied dealings that we have with each other. How do we know what unauthorized access is or particularly exceeding [authorized] access is on the Internet? The normal mode for the Internet is that I can send you an HTTP request and you're going to respond to that request. That's the way the web works - so if you are running an HTTP server, how can it be unauthorized access for me to access that server unless we start putting into force the provisions that you have established to try to protect that from normal default mode that it’s open to everybody?

The web in particularly was never designed to be an exclusive devise. Passwords were something that was added to it and not always something that would be in it when it was

---

5 642 F.3d 781 (9th Cir. 2011).
designed. Berners-Lee or Sir Berners-Lee these days, who designed the whole thing and very nicely gave it to us for free - his idea was to openly and freely share information so that there would be no technological interference with the exchange of information. It was only many years after he developed the HTTP program that people started saying “but I don't want to share this information with everyone.”

So where do we put the burden? Is that a burden that is appropriately on the entity that's trying to say it’s secret or is that a burden that puts a duty on any of us if we go that we better read those stupid license agreements? If we do anything that's not specifically authorized in those license agreements then we are committing a criminal act. I think that's a very, very difficult problem. I'm not sure it's one that is resolvable in courts. So how’s that for not answering your question?

JHTL: Thank you again professor; I really enjoyed the book and greatly appreciate your time.