Foreword

Cyber Crime and the Victimization of Women: Laws, Rights and Regulations, is a unique and a very important contribution to the literature analyzing various aspects of cyber crime. This book deals directly with an issue that is usually addressed only interstitially, i.e., as an incidental aspect of a particular cyber crime case or a particular cyber crime issue.

Cyber crime against women has all of the characteristics that define cyber crime as a general phenomenon, e.g., online, often anonymous communication, messages, and other tactics that are designed to inflict "harms" of varying types and degrees on the victims and perpetrators who, for a variety of reasons, are unlikely to be identified and / or punished for the injury they inflict. Cyber crime against women tends to involve additional characteristics that distinguish it in varying ways from generic cyber crime.

As you will see from the following chapters, women are the primary targets of cyber crimes such as online harassment, stalking, and / or bullying. The behavior at issue in these crimes can involve the use of emails and / or social networking sites to bombard the victim or the victim's co-workers and family with messages that falsely accuse the woman of engaging in offensive and / or embarrassing conduct. The behavior can also involve posting nude photographs of the victim online, photographs that were either taken while the two were involved in an intimate relationship or that have been altered to make it appear that the woman posed nude when she did not.

These hostile behaviors can have devastating consequences for the victims. Two years ago, I did a presentation on Internet defamation and invasion of privacy at a law enforcement conference. Afterward, a prosecutor approached me and told me of a particularly heinous case she had handled recently: Jane Doe and her sister Julie Doe were twins. Jane was married with two children and had a job she enjoyed, both for the work itself and for the close relationships she had with her co-workers. Julie tended to live on the "wild side." Her exploits were notorious, at least among her family and friends. For some reason, someone posted a photograph of Julie, in which she was nude and in a compromising situation with an unidentified male, on a website and included a caption that identified the woman in the photograph as Jane Doe. The person who did this then sent emails to Jane's family, friends, and co-workers that directed them to the website on which the photo of Julie-identified-as-Jane was posted.

By the time Jane learned about the photo and the emails, she had been fired from her job. Neither her employer nor her co-workers would believe her denials that the person in the photograph was her and her claims that it was, in fact, a photograph of her sister, Julie. Her employer and former co-workers had "seen the photograph for themselves" and were certain they recognized the woman in it as Jane Doe. Therefore, Jane lost her job and all of the people she once worked with told others in the small city in which Jane lived about the site and about Jane's photograph. The visual lie the anonymous perpetrator

of this cyber crime created ripples through the community, seriously damaging Jane's once impeccable reputation.

And the virtual lie almost ended her marriage. We might think that Jane's husband, who knew Julie and knew about her exploits, would instantly realize that the photograph was of Julie, not his wife Jane. However, he did not. He blindly believed the photograph was, in fact, of his wife and persisted in that belief for some time, despite Jane's pleas for him to believe her and to assess the situation rationally, given what he knew of her sister. He finally relented and decided not to file for a divorce, but the relationship between the two was still strained.

Jane came to the prosecutor I spoke to, asking her to find the person who had posted the photography and prosecute him or her. The prosecutor told Jane that the U.S. State in which they lived had a sixty-year old statute that made defamation a crime. The prosecutor told Jane she believed she could use the statute to prosecute the person who posted the photograph for criminal defamation, since the statute did not limit the conduct at issue to the use of traditional print media, such as a newspaper or magazine. That was the good news. Then the prosecutor told Jane the bad news: She was not at all sure her investigators would be able to identify the person responsible for posting the photograph, and even if they were able to identify him or her, criminal defamation under that State's statute was a misdemeanor, which meant that if the person was convicted the punishment would almost certainly consist only of a small fine and perhaps a period of probation or community service. In fact, the investigators were never able to find out who posted the photograph.

The above-mentioned relatively simple case illustrates the problems and policy issues you will read about in this book. You will learn more about cases like this that are handled in the United States; you will also learn about how they are handled in several other countries. Most importantly, perhaps, you will be able to review a model charter that is designed to improve how governments respond to cyber crimes against women.

Susan W. Brenner
NCR Distinguished Professor of Law and Technology
University of Dayton School of Law, Dayton, Ohio, USA
April 2011

Susan W. Brenner *is NCR Distinguished Professor of Law and Technology at the University of Dayton School of Law, USA. She specializes in two distinct areas of law: grand jury practice and cyberconflict, i.e., cybercrime, cyberterrorism, and cyberwarfare. A renowned cyber crime scholar, Professor Brenner has spoken at numerous events, including two Interpol Cybercrime Conferences, the Middle East IT Security Conference, the American Bar Association's National Cybercrime Conference, and the Yale Law School Conference on Cybercrime. She has also spoken at a NATO Workshop on Cyberterrorism in Bulgaria and on terrorists' use of the Internet at the American Society of International Law Conference. She was a member of the European Union's CTOSE project on digital evidence and served on two Department of Justice digital evidence initiatives. Professor Brenner chaired a Working Group in an American Bar Association project that developed the ITU Toolkit for Cybercrime Legislation for the United Nation's International Telecommunications Union. She is a senior principal for Global CyberRisk, LLC. She has published a number of law review articles dealing with cybercrime. Her books, Cybercrime: Criminal Threats from Cyberspace (Praeger, 2010), and Cyberthreats: the Emerging Fault Lines of the Nation State (Oxford University Press, 2008) are significant contributions to the field of Cyber Criminology and Cyber Laws. She also writes a blog, CYB3RCRIM3.*