

# Jennifer Stisa Granick

## Stanford Law School



BLACK HAT BRIEFINGS

### Top Ten Legal Issues in Computer Security

This will be a practical and theoretical tutorial on legal issues related to computer security practices. In advance of the talk, I will unscientifically determine the “Top Ten Legal Questions About Computer Security” that Black Hat attendees have and will answer them as clearly as the unsettled nature of the law allows. While the content of the talk is audience driven, I expect to cover legal issues related to strike-back technology, vulnerability disclosure, civil and criminal liability for maintaining insecure computer systems, reverse engineering, the Digital Millennium Copyright Act, trade secret law and licensing agreements.

*Jennifer Stisa Granick joined Stanford Law School in January 2001, as Lecturer in Law and Executive Director of the Center for Internet and Society (CIS). She teaches, speaks and writes on the full spectrum of Internet law issues including computer crime and security, national security, constitutional rights, and electronic surveillance, areas in which her expertise is recognized nationally.*

*Granick came to Stanford after almost a decade practicing criminal defense law in California. Her experience includes stints at the Office of the State Public Defender and at a number of criminal defense boutiques, before founding the Law Offices of Jennifer S. Granick, where she focused on hacker defense and other computer law representations at the trial and appellate level in state and federal court. At Stanford, she currently teaches the Cyberlaw Clinic, one of the nation's few public interest law and technology litigation clinics.*

*Granick continues to consult on computer crime cases and serves on the Board of Directors of the HoneyNet Project, which collects data on computer intrusions for the purposes of developing defensive tools and practices and the Hacker Foundation, a research and service organization promoting the creative use of technological resources. She was selected by Information Security magazine in 2003 as one of 20 “Women of Vision” in the computer security field. She earned her law degree from University of California, Hastings College of the Law and her undergraduate degree from the New College of the University of South Florida.*



Top Ten Legal Questions\*  
Black Hat Las Vegas 2005  
Jennifer S. Granick

1. Is it legal to sniff wireless networks?
2. What is the potential civil or criminal liability for those who operate open wireless networks?
3. How did the USA PATRIOT Act change computer crime investigation and prosecution?
4. What is the Computer Fraud and Abuse Act and how does it affect civil and governmental investigations of computer security breaches?
5. What are the legal issues surrounding honeynets?
6. Is strike-back legal?
7. When are computer logs and other digitally generated records admissible as evidence?
8. Is there a risk of civil or criminal liability for maintaining insecure computer systems?
9. Is reverse engineering legal?
10. How do I know when I need to talk to a lawyer?

\*Questions subject to change, but feel free to ask your questions during or following the talk. This talk is intended for informational purposes only. The talk is not intended to be, nor should it be interpreted as, legal advice or opinion. Neither the talk nor any information conveyed during the question and answer period creates an attorney-client relationship or any other relationship with the speaker.

Contact information:  
Executive Director, Center for Internet and Society  
Stanford Law School  
jennifer @ law.stanford.edu  
<http://cyberlaw.stanford.edu/>

