

## Agreed Statement of Facts

Sundance Law, a Professor of Engineering and Applied Science at Caltech, teaches a popular course on Digital Protection. Each term he divides his class into halves. Students in the first group are tasked with devising technological protection measures, such as encryption of digital content. Those students (“TPM” group) are then paired with counterparts in the other section, whose mission is to hack those technologies (“Defeat” group). Student work is posted on a course web site for comment and testing by other students.

During the Fall, 2003 term, Dimitry Skylore was assigned to the TPM group. He developed an anti-copying system that protected both access to and use of digital content. Skylore’s system employs both content encryption and copy control information (“CCI”) to implement permissions (so-called “digital “rights management” or DRM) in the underlying content. The CCI would be embedded in the encrypted content stream and specify whether it could be copied and, if so, how many times.

Skylore’s counterpart in the Defeat group was John Johnson. When Johnson read Skylore’s TPM description, he immediately saw a way around it. Johnson’s circumvention idea had two parts: First, he needed to decrypt the content stream and the embedded CCI. Once he had access to the CCI, he would then set the permission to infinite copies. The combination of these two features would render underlying content completely accessible for copying, distribution and playback.

Of course, decryption of Skylore’s underlying content and embedded CCI could present a problem. Skylore used 56-bit encryption, so significant computing power would be necessary to break it. It could be done either by brute force (trial and error of vast numbers of keys), or by finding an algorithm to reduce the encryption search space. Johnson did not have enough computing power at his disposal to crack Skylore’s encryption in any event.

But Johnson realized that many computers working in concert could provide the necessary computing power. If he could access the unused processing power of thousands of individual computers linked over the Internet, he could, in essence, assemble a large virtual computer. This is the idea behind [SETI@Home](#) and other distributive computational programs that run in the background on linked computers. So Johnson put up his distributional program on the class web site. This allowed cooperating users to each take a piece of the decryption problem and contribute to the solution. He sent a notice to Caltech students who, collectively, cracked Skylore’s encryption algorithm within 24 hours. Johnson posted the decryption key on the web site, along with his resume. He was confident that his program would help him land a lucrative consulting contract to help him pay tuition costs.

Prof. Law gave Johnson an A- for his work. Although changing the CCI permission set was somewhat obvious, the web-based collaborative decryption system was novel and useful in a variety of situations. In fact, Law noticed that Skylore’s TPM project was similar to the “5C” Broadcast Flag technology under development by a consortium of entertainment and

consumer electronics companies. The flag is a DRM system recently mandated by the FCC for consumer “demodulator products” (i.e., digital tuners) in television sets and other video receiving equipment,<sup>1</sup>

Prof. Law posted a few seconds of 5C encrypted video on Johnson’s web site and, sure enough, within a day the correct decryption key was found, allowing Law to copy a clear version of the movie. Word spread quickly that Johnson’s web site could be used to decrypt protected media and circumvent DRM systems. The web site is experiencing a lot of activity as college students throughout the country are logging on to obtain decryption keys.

Content producers and owners of copyrighted materials are alarmed about Johnson’s web site and decryption method. They see it as a cheap and easily used means of circumventing TPMs they use to protect video content. They could render Johnson’s system ineffective, at least temporarily, by using more robust technologies, but that would simply provoke additional hacking efforts in Law’s class and worldwide. So, they’ve decided to take a principled and aggressive approach.

The Recording Industry Ass’n of America (RIAA), the Motion Picture Ass’n of America (MPAA), and Intel (co-inventor of “5C” technology), banded together and persuaded the U.S. Department of Justice (DOJ) to bring criminal charges against Johnson, Law, Caltech and its President, Daniel Baltimore. In *U.S. v. Baltimore*, the government seeks criminal sanctions against defendants for violating the DMCA. DOJ offered to drop charges in exchange for Caltech removing Johnson’s website and prohibiting Prof. Law from teaching students how to decrypt “digital rights management devices or commercial encryption technology now in use or development.” The university responded that it would be compromising academic freedom by complying with the government’s demand.

All defendants have moved to dismiss the indictment on the grounds that the DRM/CCI device is not “effective” within the meaning of the DMCA. Dr. Baltimore, Caltech and Prof Law have also moved to dismiss the charges against them on First Amendment Grounds, and that there can be no vicarious criminal liability in this case.

The federal judge assigned to the case has set a hearing date of May 21, 2004, at which time he will hear argument of counsel and receive oral and written testimony by expert witnesses.

All names have been (slightly) changed to protect the innocent.

---

<sup>1</sup> See CFR § 73.9003 Compliance Requirements for Covered Demodulator Products: Unscreened Content.