Professor Wendy Seltzer
Information Privacy
Spring 2006

Final Examination

Instructions: This exam booklet has four (4) pages. Please be sure you have all four pages.

Please read the questions carefully. There are two questions; the first is worth 2/3 of the exam grade, the second 1/3. You have eight hours to complete the exam. Please allocate your time and effort accordingly.

This exam is open book and take-home. Please base your answers on assigned readings and class discussions. You may bring in pre-existing outside knowledge, but you may not do Internet or Lexis / Westlaw searches for additional information once you have received the examination questions. (Such searches are unlikely to help you in any event.) Of course, you may not consult with anyone else during the exam.

Word limit: 3000 words. Courts enforce word limits and so will I. Your exam must be no longer than 3000 words, including any footnotes or endnotes (approximately 15 pages double-spaced). **Please include a word count at the top of your document.** I will spot-check word counts and will stop reading after 3000 words.

Anonymity. Your name should not appear anywhere on the exam. Each page should have your exam number and page number.

Good luck! Thanks for a great class.

Question 1: The Sound of Spyware

The Monster Music Group ("MMG"), a major recording label, has decided to release albums online. To combat piracy, MMG does not release the music as MP3 files, but as encoded .mus files, which will play only in the MediaPlay application downloaded from MMG's website.

At the MMG website where they download MediaPlay, users can click a link labeled "[Privacy Policy]." The privacy policy tells users that:

> "Monster Music Group and its artists respect your privacy. When you browse our website, we collect only anonymous usage data. We do not use web bugs.
>
> When you purchase music, we collect personal information including your name, address, and billing details. We do not share this information with third parties, except as necessary to process your order and bill you.
>
> The MediaPlay application also collects anonymous usage data about the media files you play. We may use this information to improve your listening experience by suggesting other songs and videos we think you might like."

The MediaPlay application can play both .mus files and files from other common audio and video formats such as MP3 and QuickTime. Similar to iTunes and WinAmp, it enables users to catalogue and create playlists of all their audio and video, not just MMG's music. (It reads the filename and metadata to guess at what music is being played, or allows users to enter their own identification.) Because MMG distributes music from many popular bands in .mus format, the MediaPlay application becomes popular very rapidly. Many users adopt it for all their entertainment media.

When playing audio files, MediaPlay displays advertisements, which often include clickable links to music stores selling albums by the same artist currently being played. Invisible to its users, MediaPlay also keeps a list of all the files played and periodically transmits this list to MMG to obtain new advertisements.

Jane Hacker, after noticing that her computer seems to be making frequent Internet requests while MediaPlay is running, manages to decipher the data stream being sent to MMG. Jane sees that this data stream contains not only the names of the videos and songs she has watched and listened to, but also her name and address. She posts an article to her weblog saying "MediaPlay is Spyware! It reports on you – by name – and

sends records of your listening habits to Monster Music Group." The blog is soon filled with angry comments against MMG, and the story spreads to other websites and newspapers.

Things get even worse when an MMG employee loses a laptop. Shortly thereafter, popular gossip weblog StarStalker begins a series of features entitled "What the stars listen to," inviting readers to "Get the intimate details on your favorite celebs' listening habits, straight from the records of Monster Music Group!" StarStalker says "someone left this set of playlists in our mailbox."

One StarStalker post, "Venice's hard drive is hard core," features a playlist for actress Venice Radisson that includes the titles of many explicit pornographic videos. Another post, about pop singer Johnny Revolting, claims "Recordings reveal Revolting's racism," showing a playlist filled with music from Aryan Resistance, a racist and anti-Semitic group.

MMG customer support is overwhelmed with angry messages from customers. Already, a class action law firm has posted a notice to its website saying "Harmed by MMG's MediaPlay??? Click here!!" soliciting potential plaintiffs to fill in a contact form. One of the celebs whose playlist was featured on StarStalker has threatened to sue "everyone connected with this."

Who might bring privacy-related claims against whom here? Describe the possible causes of action and evaluate their likelihood of success based on the facts given. Since we often head into litigation without knowing all the facts, if you make additional reasonable assumptions, spell out your assumptions and the questions you might ask to verify those assumptions. Consider whether MMG should be concerned about complaints from parties not listed above.

Finally, in a separate section, imagine that you have been brought in as chief privacy counsel to MMG to help them understand the privacy issues. How might you advise the company to proceed?

Question 2: The Computer Never Forgets

You are a new privacy attorney in the Justice Department's Office of Legal Counsel, the office responsible for advising the administration and Attorney General on the law and on the constitutionality of proposed legislation. You were hired specifically to help the Justice Department understand and respond to Americans' privacy concerns.

Your boss, the Attorney General, tells you he thinks that it would be very helpful to law enforcement if Internet service providers (ISPs) were required to keep records of all users and all communications going through their facilities. Law enforcement could then use those records to help investigate crimes and track suspected terrorist activity. Currently, while law enforcement can ask ISPs to preserve records they have already generated, it gets nothing if the ISPs have not logged activity or have deleted logs by the time the government request arrives.

The AG thinks that the utility of this recordkeeping would be enhanced further by "know your customer" requirements for ISPs. The AG would like all ISPs – including libraries and Internet cafes – to keep records identifying the actual person who buys or uses an Internet connection, so that law enforcement doesn't find itself following a trail of collected information only to get to "the person who paid $2 in cash for an hour of Internet access at Ted's coffee shop."

Before he begins drafting a legislative proposal, the AG wants your advice. He asks you to write candidly about the strengths and weaknesses of his proposals, saying the memo will be confidential, protected from disclosure under FOIA by the deliberative process and attorney-client privileges. Technologists on the staff will evaluate the technical feasibility of the proposals, so you need not address those.

The AG's questions include:

- Are the recordkeeping and disclosure requirements he proposes constitutional? (Assume that any ISP compensation issues can be worked out.)
- What are the most significant intersections with current law? Would you recommend amending existing statutes to protect privacy or to make this proposal more effective?
- As a policy matter, is mandatory data retention a good idea? What are the privacy tradeoffs?