Amazon.Com LLC v. Lay, **Case. No. C10-664 (W.D. Wash. Aug. 12, 2010). This is a declaratory judgment action brought by Amazon against the secretary of the North Carolina Department of Revenue, which sought to compel Amazon to disclose the names and addresses of Amazon's customers in the State. The court granted the motion of North Carolina residents to intervene pursuant to Rule 24(a) finding, among other things, that their First Amendment rights may be chilled by any disclosure. The court also allowed the intervenors to proceed anonymously as "their privacy interests outweigh any prejudice to the parties or the public's interest in knowing their identities."**

Chrysler Corp. v. United States, **604 F.3d 1378 (Fed. Cir. May 14, 2010) (*per curiam*). The Court of Appeals denied Chrysler's requests for a panel rehearing and a rehearing *en banc.* Chrysler had sought the refund of export taxes that had been declared unconstitutional. However, the government agency charged with collecting the taxes declared that its electronic records were unreliable (based on "almost a 10 percent error rate") for taxes paid before July 1, 1990 and required independent evidence for refunds, which Chrysler could not provide. Dissenting from the *en banc* denial, Circuit Judge**

Newman took the court to task. The court, deferring to administrative rulemaking, had reversed the presumption of correctness of official government records. "Applying the normal presumptions and burdens, a reasonable protocol for reliance on official records that the government believes to be flawed might be established."

Crispin v. Christian Audigier, Inc., **Case No. CV 09-09509 MMM (JEMx) (C.D. Ca. May 26, 2010). In this action arising out of an alleged oral contract between the parties, the defendants subpoenaed social networking websites. The plaintiff's motion to quash was denied by a magistrate judge. On a review of that denial, the district court distinguished between "remote computing service" and "electronic communications service" providers under the Stored Communications Act. The court also held that the party plaintiff had standing to challenge the subpoenas had a "personal right" to the information in issue and rejected the defendants' argument that *civil* subpoenas are authorized by the Act. Then, after concluding that the web sites were ECS providers under the Act, the court addresses the question of information sought by the subpoenas (private messages and postings) was in "electronic storage." Noting that the Act gives two definitions of that phrase, the court distinguished between email, on the**

one hand, and postings or comments, the latter being "not protectable as a form of temporary, intermediate storage."

In re: Anonymous Online Speakers, **No. 09-71265 (9th Cir. July 12, 2010). The defendant in this civil litigation had been accused of orchestrating an Internet "smear campaign via anonymous postings and videos." Three anonymous speakers sought mandamus relief from an order requiring the disclosure of their identities. The plaintiff filed a cross-petition to compel the disclosure of the identities of two other anonymous speakers. The Court of Appeals denied both petitions. In doing so, the court addressed First Amendment protection for anonymous speech and observed that the Internet was the "latest platform" for such speech. "The right to speak, whether anonymously or otherwise, is not unlimited, however, and the degree of scrutiny varies depending on the circumstances of the type of speech at issue." The Court of Appeals held that the speech in issue was commercial in nature and canvassed various standards applied to balance the First Amendment privilege for anonymous commercial speech with the need for discovery. Having done so, the Court of Appeals concluded that the trial court had not committed clear error in the balancing test which it had employed and which had established a "high hurdle for disclosure." The Court of Appeals also noted that the parties had entered into a protective order which established various levels of**

disclosure. On the cross-petition, the Court of Appeals held that it fell within "the category of a garden variety discovery dispute.

In re Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, **No. 08-4227 (3d Cir. Sept. 7, 2010). In this case of first impression, the Court of Appeals interpreted Section 2703(d) of the Stored Communications Act, which requires "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic information, or the records or other information sought, are relevant to an ongoing criminal investigation" for an order to issue. A magistrate judge, in an opinion joined in by her colleagues and affirmed by the district court, held that this language required the Government to show probable cause for the issuance of an order compelling disclosure by a cell phone provider of "historical cell phone data" of a customer. The appellate court rejected this interpretation of Section 2703(d). The court did hold, however, that the Act gave a magistrate judge discretion (to be "used sparingly") to require the Government to proceed by warrant, which would require probable cause.**

Ostergren v. Cuccinelli, **No. 09-1723 (4th Cir. July 26, 2010). The plaintiff is a privacy advocate. To further that advocacy she posted on a website land records from Virginia that included individual Social Security numbers of public officials. After being threatened with prosecution under a Virginia statute that prohibited the intentional communication of Social Security numbers, she commenced this action for declaratory and injunctive relief. The district judge declared the statute unconstitutional and entered a permanent injunction against prosecution of the plaintiff for publication of the officials' numbers. Both the plaintiff and the Commonwealth appealed. The Court of Appeals held that the plaintiff had engaged in protected speech under the First Amendment. The court then balanced the plaintiff's free speech rights against the "considerable privacy interest" of the individuals whose numbers had been published. The court noted that the privacy interest at stake was not the secrecy of information but, rather, *control* over how information might be used or handled. Balancing those interests (as well as the ability of Virginia to avoid the *initial* disclosure of the numbers), the Court of Appeals affirmed the issuance of the injunction. On the plaintiff's cross-appeal, the Court of Appeals declined to address her contention that the First Amendment barred prosecution for publication of numbers secured from websites**

of other States. The court did hold, however, that the injunction was not properly "tailored:" It should have protected the plaintiff from prosecution for publication of any numbers found in Virginia land records, be those of private individuals or out-of-state public officials who had property transactions in Virginia. The Court of Appeals remanded for further proceedings and development of the record.

United States v. Maynard, **No. 08-3030 (D.C. Cir. Aug. 6, 2010). After being convicted for drug trafficking, two defendants appealed. One argued that his Fourth Amendment rights were violated by the Government's warrantless installation in the defendant's vehicle and use of a Global Positioning System ("GPS") device to track his movements continuously over a month. As characterized by the Court of Appeals, at issue was "prolonged visual surveillance." The court held that the defendant's movements were not exposed to the public: "the whole of a person's movement over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements in not just remote, it is essentially nil." The court also rejected the argument that the defendant's movements were *constructively* exposed: "The whole of a person's movements … is not constructively exposed to the public because … that**

whole reveals far more than the individual movements it comprises." The court held that the defendant had a *reasonable* expectation of privacy in his movements over a month noting, among other things, the cost of human surveillance over time. (*And referencing a scary technology known as a GPS-enabled dart*). The court concluded that that the installation and use of the GPS device constituted an unreasonable search in violation of the Fourth Amendment. This error not being harmless, the defendant's conviction was reversed.