

Congressional Internet Caucus Advisory Committee Privacy Task Force
Briefing Book Submission
April 19, 2001

SUBMITTED BY: The Competitive Enterprise Institute

AUTHOR AND CONTACT: Solveig Singleton, Senior Analyst, Project on
Technology Innovation, (202) 331-1010 or ssingleton@cei.org

SECTION: Introduction

SUBSECTION: The Purpose of Choice Principles

A Critical Look at Purposes Underlying the Choice Principle

The Choice Principle as a substitute for market mechanisms of consent and accountability, for information held by the government. The principle that consumers should be able to choose how information about them was introduced into US law during the debate leading up to the Privacy Act of 1974¹—a privacy law intended for information held by *government*, particularly medical information. Because one rarely has a choice as to whether turn over information to government in the form of a driver's license application, a tax form, or a Medicare record, making a special provision for choice when citizens are dealing with the government makes sense at least on a superficial level (more so for health records than for public records). The government has unique powers to control the police and the courts that the private sector lacks. And it is hard to hold government employees accountable for misuses of information. Of the hundreds of IRS employees caught in the late 90s snooping through the tax forms of neighbors and celebrities, only a handful were fired. And the aggrieved citizens whose tax forms were perused in this casual manner had no choice but to deal with the IRS again the following year. (By contrast, a clerk in a private-sector law firm caught leaking confidential client information is likely to be fired, and there is possibility that the firm will lose its client to another firm).

The principle of choice has since been uncritically applied to the private sector, but there remains a serious question as to its appropriateness outside of the context of medical information or information held by government.

The Choice Principle as establishing a right to control one's personal information—and creating conflict with the free flow of information. As applied to the private sector, a key purpose of the choice principle put forward by its defenders is the idea that people ought to control information about themselves—even after that information has been voluntarily shared with others. The idea that people should not have to give out information about

¹Kathleen A. Frawley, "Federal Legislation on Confidentiality: Possibility or Insurmountable Challenge?" *Journal of AHIMA*, March, 1999, available at <http://www.ahima.org/journal/features/feature.9903.1.html>

themselves if they do not want to is uncontroversial. However, the claim that one ought to retain a right to control information *after* it has become known to others in the ordinary course of a transaction or relationship is a much more radical claim (assuming that the company has not made a promise to keep the information confidential). It essentially amounts to claim of ownership in that information, equivalent to a drastic expansion of copyright or defamation law. In this sense, the choice principle verges on a kind of censorship, essentially giving the chooser a veto power over other's rights to learn about him and communicate facts and opinions concerning him to others. In this sense, the choice principle comes squarely into conflict with principles of free speech.²

Choice As Consumer Protection or Crime Prevention. Another purpose of the choice principle might be to allow consumers to control the risks associated with the gathering of information about themselves, for example, the risk of credit card fraud, identity theft, or stalking. But the choice principle would not serve this purpose very well. First of all, there is little or no evidence that information gathered by legitimate companies for ordinary purposes like marketing presents any real harm to consumers (and there is growing evidence of benefits to consumers). Criminals are just as or more likely to find information from phone books, newspapers articles, utility bills or other items fished out of dumpsters or mailboxes; sometimes, identity thieves turn out to be vengeful relatives or roommates with access to the victim's purse or papers. It would be much more effective to address problems like stalking or identity theft by developing new law enforcement mechanisms to better enforce existing laws against these crimes.³

One might add that the choice principle is necessary to protect human dignity or autonomy. This, however, is a purpose so vague as to be almost meaningless. How exactly is human dignity harmed by a company's seeking to learn more about its customers' preferences by studying their behavior? It is difficult to believe that Americans have become so pathetic as to require federal protection from Safeway's knowing that they bought lettuce, whether or not Safeway passes that information on to a salad bowl seller.

² See, e.g. Solveig Singleton, "Privacy Versus the First Amendment: A Skeptical Approach," XI Fordham L. J. 97 (2000); Eugene Volokh, "Personalization, Privacy, and the First Amendment," *published in The Future of Financial Privacy* (Washington, D.C.: CEI 2000).

³ Rep. James Leach, "Identity Theft Vexes Lenders, Consumers," *Mortgage Servicing News*, November, 2000, p. 4. ("Despite [the] profusion of Federal and State statutory authority . . . there is little evidence that law enforcement agencies have made combating this crime a priority. A recurring theme at least week's hearing was the difficulties encountered by victims of identity theft and the financial institutions that bear the losses in obtaining redress, either because financial thresholds established by prosecutors' offices have not been met or because resources are simply being directed elsewhere."); see Jackie Hallifax, "Task Force Grapples with Privacy Issues in Technology Age," *The Associated Press State and Local Wire*, December 15, 2000 (outlining better enforcement methods for identity theft).