Testimony of

Wayne Crews
Vice President for Policy/Director of Technology Studies
Competitive Enterprise Institute

Before the Committee on Commerce, United States Senate

Privacy Implications of Online Advertising

Wednesday, July 9, 2008
10:00 AM

Russell Senate Office Building 253

The Competitive Enterprise Institute (CEI) is a non-profit public policy research foundation dedicated to individual liberty, limited government, and markets. We appreciate the opportunity to discuss policy issues surrounding online advertising.

Privacy dilemmas are inevitable on the frontiers of an evolving information era, but CEI maintains that competitive approaches to online privacy and security will be more nimble and effective than rigid political mandates at safeguarding and enhancing consumer well-being, facilitating commerce and wealth creation, and even contributing to the rise of the anonymous approaches to commerce we'd like to see.

The Rise of Privacy and Cybersecurity as Public Policy Issues

The marvelous thing about the Internet is that one can contact and learn about anyone and anything. The downside is that the reverse is often true. The digital information age—against a backdrop of rising globalization—offers consumers unprecedented access to news, information, democratized credit and much more. Anyone may collect and share information on any subject, corporation, government—or in many cases, other individuals.

Companies from retailers to search engines to software makers all collect consumer data—enough to fill vast server warehouses. Of course, Web sites have long collected and marketed information about visitors. The latest twist is that behavioral marketing firms "watch" our clickstreams to develop profiles or inform categories to better target future advertisements. Unarguably beneficial, the process stokes privacy concerns. Fears

abound over the data's security; is any of it personally identifiable? If not, can it conceivably become so? Will personal information fall into the wrong hands? Will it become public? And if a breach occurs, who's punished? While Capitol Hill, beltway regulators or state governments are seen often as the first line of defense, regulatory and legislative proposals, much like the anti-spam law, can fall short of success. Aspirations can exceed actual legislative capability.

Clearly, as a technological phenomenon, mass transactional data tracking and collection are here to stay; and with nascent technologies like biometrics that could fully authenticate users on the horizon, the debates will only intensify.

Along with behavioral advertising, new data-mining and biometrics technologies promise higher levels of convenience and, ultimately, more secure commerce online. Beyond the "merely" commercial, the technologies also hint at greater physical security in the "homeland" and in our workplaces via authentication.

On the upside, online advertising enables today's familiar subscription-fee-free cornucopia of news and information, and the free soapbox enjoyed by bloggers worldwide. It's become cliché to note the commercialized Internet is one of the most important wealth-creating sectors and democratizing technologies ever known. Benefits to society range from frictionless e-commerce, to the democratization of privileges once available only to the rich, to a megaphone for all.

This online bounty has also brought real and imagined privacy vulnerabilities to the forefront, ranging from personal identity theft to exposure of private thoughts and behavior online. Once, we could contend merely with nuisances like spam, cookie-collection practices and the occasional spyware eruption. Since policies today are being formulated in the context of a post-Sept. 11 world, cybersecurity and computerized infrastructure access and security join routine privacy as prime policy issues. Adding complexity is the noted emergence of biometric technologies and highly engineered data mining that could alter the future of behavioral marketing. Thus we must contend not just with run of the mill commercial aspects of privacy policies, but with national security themes and what some consider a dangerous new surveillance state.

The question is, do newfangled data collection techniques threaten fundamental expectations of privacy, and in the case of government data collection, even liberty itself?

What principles distinguish between proper and improper uses of personal information, and what policies maximize beneficial e-commerce and consumer welfare? Business use of behavioral advertising can be irritating, but many have made peace with advertisers' using personal information. One-size-fits-all privacy mandates will undermine e-commerce and the consumer benefits we take for granted. Sweeping regulations can especially harm start-ups that lack the vast data repositories already amassed by their larger competitors. Our policies should be consistent with tomorrow's entrepreneurs (and consumers) starting businesses of their own to compete with the giants of today.

Thus, privacy policies need to be filtered through the lens of the entire society's needs. We must consider the impact on (1) consumers (2) e-commerce and commerce generally (3) broader security, cybersecurity, homeland security and critical infrastructure issues, and finally (3) citizen's 4th amendment protections.

Happily the prospect of billions in economic losses from mistakes incentivize the market's efforts to please consumers and safeguard information and networks.

Web Functionality Continues to Unfold

The recent emergence of behavioral advertising reinforces the easily forgotten reality that there's more to the Internet than the "Web" at any given juncture; it's only 2008, and there are doubtless more commercially valuable avenues for marketing yet to be discovered in the decades ahead. Targeted, behavioral and contextual advertising make use of heretofore unexploited underlying capabilities of the Internet, possibilities that hadn't yet occurred to anyone else, just as the original banner ad trailblazers first did years ago—and, yes, just as the spammers did.

At the Outset: Policy Must Distinguish Between Public and Private Data

Parameters are needed to talk coherently about the treatment of individual's data. Information acquired through the commercial process must be kept separate from that extracted through government mandates. Similarly, private companies generally should not have access to information that government has forced individuals to relinquish (what one might call the "Social Security" problem). Private industry should generate its own marketing-related information (whether "personally identifiable" or not), for purposes limited by consumer acceptance or rejection, rather than piggyback on government IDs. Confidentiality is a value, and should be a competitive feature.

Conversely, for any debate over behavioral advertising to make sense, corporate America needs to be able to make credible privacy assurances to the public. People need to know that the data they relinquish is *confined to an agreed-upon business, transactional or record-keeping purpose*, not incorporated in a government database. If regulators end up routinely requiring banks, airlines, hotels, search engines, software companies, Internet service providers and other businesses to hand over private information (in potentially vulnerable formats), *they will not only undermine evolving commercial privacy standards, including behavioral, but make them impossible*, Government's own information security practices is the elephant in the room when it comes to contemplating e-commerce sector's stance with respect to privacy. It's all too easy to give the online marketing industries a black eye and risk turning society against the technologies, and ensure regulation and politicization. Private data and public data policies are potentially on a collision course, but need not be.

The benefits that personalization brings, like easier, faster shopping experiences, are in their infancy. Sensible data collection improves search, communication, ability to

innovate, U.S. competitiveness—all the things we associate with a well-functioning economy and evolution in healthy consumer convenience and power.

Privacy Legislation: Premature and Overly Complex

In contemplating government's role with respect to privacy and information security, we must recognize the realities of differing user preferences that preclude one-size-fits-all privacy and security policy. Online, there are exhibitionists and hermits. Some hide behind the equivalent of gated communities; others parade less-than-fully clothed before personal webcams.

Note how we work ourselves up into a lather: policymakers were concerned about privacy when ads were *untargeted and irrelevant* (spam); now a solution—behavioral and contextual marketing—makes ads relevant, and we're hand-wringing about privacy there too. Incidentally, spam was framed as a privacy problem, but in reality the spammer didn't typically know who you were. Likewise, a positive early development in behavioral advertising is that personally identifiable information is not always crucial to the marketer (although sensible uses of personally identifiable information should not be thwarted). Too often, the complaint seems to be *commerce as such.* For example, the Federal Communications Commission recently decided to investigate the "problem" with embedded ads in TV programming.[1]

Policy should recognize privacy is not a single "thing" for government to protect; it is a *relationship* expressed in countless ways. That relationship is best facilitated by emergent standards and contracts—like the Network Advertising Initiative's behavioral advertising principles[2] that predate the Federal Trade Commission's late 2007 principles[3]—and in emergent market institutions like identity theft insurance. Apart from varied privacy preferences, any legislative effort to regulate behavioral advertising gets exceedingly complex:

- If online privacy is regulated, what about offline?
- Should behavioral advertising be opt-in or opt-out? (Why and when?)
- Who defines which advertising is "behavioral"?
- What is the legislative line between sensitive, and non-sensitive, personally identifiable information?
- Should the federal government pre-empt state privacy laws?
- Will the privacy rules apply to government?
- Will government abstain from accessing or seizing private databases?
- What about *non-commercial* information collection? (Will the rules apply to bloggers? Or to Facebook activism?)

[1] Associated Press, "FCC to look into embedded advertising on TV," *MSNBC.com*. June 26, 2008. http://www.msnbc.msn.com/id/25401193/

[2] http://www.networkadvertising.org/networks/principles_comments.asp

[3] Federal Trade Commission, "Behavioral Advertising, Moving the Discussion Forward to Possible Self-Regulatory Principles," December 20, 2007. http://www.ftc.gov/os/2007/12/P859900stmt.pdf

- What about consumer harm caused by privacy legislation (Given that in the business world, most transactions occur between strangers.)
- What of practical problems of written privacy notices? (Especially given the declining importance of the desktop, the emergent web-like multi-sourced nature of web-pages themselves, smaller wireless-device screens, and the "thing-to-thing" Net that bypasses humans altogether.)
- Could disclosure and reporting mandates create a burdensome paperwork requirements detrimental to small businesses? (A privacy "Sarbanes-Oxley")
- What about the right to remain anonymous; Behavioral marketing appears to be on course to facilitate anonymous transactions; will government permit it? How should tolerance of anonymity differ in commercial and political contexts?

The Internet was designed as an open, non-secure network of semi-trusted users. Thus one interpretation of the nature of the cyberspace is that advertisers may legitimately assemble information on what is clearly a very public network that never offered any real pretense of security. But even assuming one's online pursuits can be tracked, privacy tools nonetheless are emerging, and vendors must be held to commitments. Given legislation's complications and the Internet's inherent security limitations, a rational policy prescription should be more limited: *Hold the private sector accountable to the contracts and guarantees it makes, and target identity theft and the criminals who perpetrate it.* If legislation merely does such things as send bad actors overseas, we merely create regulatory hassles for mainstream companies that already follow "best practices," and for small businesses trying to make a go of legitimate e-commerce.

As in spam debate, we face less a legislative problem than a technological one. It's true that social norms and expectations have yet to gel—but those are as varied as individuals are.

Marketing **Is Not Today's Dominant Information Collection Threat**

The emphasis on online privacy legislation could represent a case of misdirected energy. The most important information collection issues of the day are not related to mere *marketing*; rather, criminals who ignore already existing laws and will ignore any new law, are the ones creating mischief online, abusing the trust we have or would like to have in vendors. Meanwhile, *government* surveillance and information collection threaten liberties and *genuine* privacy—and one cannot "opt out." (One is reminded of the Peanuts cartoon of Snoopy sitting on his doghouse typing, "Dear IRS…Please remove my name from your mailing list."[4])

The stringent opt-in standard some seek in the behavioral marketing debate is not one government tolerates for itself. The post-Sept. 11 push for compulsory national ID cards, warrant-less wiretapping and escalating data retention mandates signify a government more inclined toward infringing privacy than acting as guarantor.

[4] http://www.freerepublic.com/focus/f-news/1384722/posts.

The rise of the information society amid a "homeland security culture" is an unfortunate coincidence, an accident, but one that colors debates over marketing that would otherwise be more pedestrian. The tendency of government to interfere with privacy practices is undeniable: Total Information Awareness, CAPPSII, and a national ID are examples of expansive government efforts that would undermine the private sector's freedom and ability to make privacy assurances in the first place.

Worse, when technology companies contract with government for information services, they would very likely request immunity for data breaches by extension of the Homeland Security Act that grants similar immunities for failed security technologies; so if markets are tempted to repudiate self-regulation and liability for privacy standards, government oversight becomes the default. The "homeland security culture" can undermine the market's entrepreneurial tendency to resolve the dilemmas created by information sharing.

Deliberations over privacy and online security should start with the recognition that government often doesn't need to protect our privacy, it needs to *allow it in the first place*. Business, whatever missteps happen in behavioral marketing, can deliver. As it stands, nobody's in any position to make ironclad security guarantees given the open nature of the Internet, but the Web is a giant research experiment, and techniques will improve. In fact, as behavioral tracking does begin to employ personally identifiable information, security benefits in ways that people will approve. The Net's governmental origins have left privacy expectations and rights somewhat ill-defined in many online contexts. But we all at times need to identify ourselves and validate the identity of others.

Consumers are Not Powerless: The Redundancy of FTC Standards

In spite the Net's vulnerabilities, consider how legislation pales compared to unforgiving competitive discipline. An old joke holds that if McDonald's was giving away free Big Macs in exchange for a DNA sample, there would be lines around the block. But consumers do care; and thanks to the Internet itself, they are hardly a voiceless mass.

Every few weeks brings new headlines about government data-handling debacles, such as governmental bodies forcing employees to carry Social Security cards on their person, or the IRS requirement that payment checks feature the SSN.[5] Confidence isn't inspired when the government's information practices lag the private sector's.

Contrast that with what happens to a careless private firm. Google and its recent mergers and alliances put it under scrutiny, but why? (Recall it was Google that in 2006 refused to hand over user search data to the Justice Department; and Google's YouTube division is now being forced by the a New York district court to hand over user viewing records in a video piracy case. Google not unsurprisingly objects.) But imagine if Google suffered a serious data breach. Consumers would lose trust, and Google could lose millions. Examples abound of consumer sovereignty, such as the backlach against Facebook's

[5] Associated Press, "U.S. Contradicts Itself Over Its Own ID Protection Advice," SiliconValley.com, July 2, 2008. http://www.siliconvalley.com/news/ci_9762027?nclick_check=1.

Beacon that cross-posted users shopping activities on friends' sites,[6] and Comcast's de-prioritizing of certain file sharing transfers. Today's Internet users are empowered to educate the world about business practices of which they disapprove. The blogosphere transforms Web users into citizen-journalists, harnessing the power of collective discontent. The result: *Companies routinely change and improve their information handling procedures without law*.

Policies proposed in the name of what consumers want or should want are all too common, as if the ideas hadn't occurred to anyone in the competitive marketplace already, or as if the markets hadn't been forced to adapt already, or as if issues weren't more complicated than the regulators suppose.

For example, the November 2007 FTC proposal on behavioral advertising offers pedestrian principles that have long been in play:[7] Paraphrasing, sites should declare that info is being collected and used and users can opt out; data should be "reasonably secured," and retained only as long as necessary; affirmative consent be given for privacy policy changes; and sensitive information should not be collected at all, or only with affirmative opt-in.

Where do the real incentives lie? Industry looks at what consumers actually want; industry often already embraces opt-in for sensitive information categories, even when the information is not personally identifiable. And if not so empowered by a benevolent vendor, users can already exercise the choice allegedly sought in privacy legislation; they can simply choose not to disclose sensitive information on certain sites, or employ privacy software that can thwart unwanted data collection and allow anonymous Web browsing. "Anonymizer" is still out there for encrypted, anonymous surfing. People can switch to "Scroogle" to disguise their Google searches; A consumer can use a dedicated tool to nullify his identity prior to a sensitive search like "HIV"; TrackMeNot can send out "white noise" search queries to disguise the real one. No mandates for choice are needed; choice is the default, whether vendors prefer it or not.

In terms of competitive enterprise, the divisiveness of a debate like behavioral marketing implies that *real market opportunities exist in providing online anonymity*. After all, despite all the hand-wringing over personally identifiable information, any given marketer doesn't necessarily need to know who *you are*, but how somebody *like you* acts. (Much like a politician seeking a vote, incidentally.) Again, the worry is less that the market is invading our privacy and more whether that anonymity will be permitted politically when it finally is available to us commercially.

"Self-Regulation" Is a Misnomer

Privacy and security need to be competitive features. We need to foster competition in reputations. And we need flexibility when the inevitable mistakes are made.

---

[6] Caroline McCarthy, "MoveOn.org takes on Facebook's 'Beacon' ads," CNet News.com. November 20, 2007. http://news.cnet.com/8301-13577_3-9821170-36.html

[7] Federal Trade Commission, 2007.

Businesses compete; and one area in which they can compete is in the development of technologies that enhance security. Washington's inclination toward regulating online consumer relationships threatens to undermine the market's catering to diverse individual privacy preferences, and hinder the evolution of competitive research and innovation in secure applications. Privacy encompasses innumerable relationships between consumers and businesses, and no single set of privacy safeguards is appropriate. While government demands information disclosure, profit-driven firms compete to offer robust privacy assurances. As businesses respond to evolving consumer preferences, stronger privacy policies will emerge.

Businesses are disciplined by responses of their competitors. Political regulation is premature; but "self-regulation" like that described in the FTC principles is a misnomer; it is *competitive discipline* that market processes impose on vendors. Nobody in a free market is so fortunate as to be able to "self regulate." Apart from the consumer rejection just noted, firms are regulated by the competitive threats posed by rivals, by Wall Street and intolerant investors, indeed by computer science itself.

Neither the government nor private sector has a spotless "self-regulatory" record, but FTC seems unconcerned about the former. Data breaches at businesses, governments and universities rose 69 percent in 2008.[8] Government can contribute to data security by ensuring that its own policies—like data sharing or data retention mandates, or sweeping subpoenas—do not interfere with competitive discipline.

Even governmental calls for self-regulation seem lukewarm. Along with the Federal Trade Commission's Principles on what personally identifiable information firms may collect, a bill in the New York state legislature would impose drastic opt-in standards, preventing companies from gathering personalized information without explicit user permission. When Microsoft bid for Yahoo this year, the Justice Department almost immediately wondered whether the combined firm would possess "too much" consumer data. Canada recently announced an investigation into Facebook's privacy protections. Now the Department of Justice is investigating the Google-Yahoo deal.[9]

Everybody's heard of Google and Microsoft, but fewer have heard of companies like Phorm and NebuAd, which present the more pertinent behavioral marketing issues; their new techniques give ISPs a dog in the fight, since online advertising is a commercial opportunity impossible for ISPs to ignore. ISPs see Google and Microsoft and they want a piece of the online advertising action too. These companies' techniques have been called spyware, but again, they incorporate the Net's underlying capabilities in novel ways, and they too are subject to competitive discipline. One's sympathies will depend upon the "ownership" status one accords to Web pages, and what one regards as online "trespass." The only certainty is a Web page today is not what a Web page tomorrow will

[8]Brian Krebs, "Data Breaches Are Up 69% This Year, Nonprofit Says," *Washington Post*. July 1, 2008. p. D3. http://www.washingtonpost.com/wp-dyn/content/article/2008/06/30/AR2008063002123.html.
[9] Peter Whoriskey, "Google Ad Deal Is Under Scrutiny," *Washington Post*, July 2, 2008. Page D1. http://www.washingtonpost.com/wp-dyn/content/article/2008/07/01/AR2008070102622.html

be. Was there ever a real reason for publishers and advertisers to think they could control everything a user saw, given the open-ended potential of software's obvious ability to route content to browsers in novel ways? At many sites, like Facebook, each page is a "Web" in its own right, containing widgets drawing information and ads from numerous sources. The debate has really only just begun, and online marketing trade groups are truly the "Battered Business Bureau." But they're battered by competitive discipline, not merely regulators

Lessons from Personally Identifiable Data Use Can Inform Future Online Security Practices

A frontier industry requires the flexibility to learn from mistakes. We must distinguish between proper and improper uses of surveillance by *both* the private and public sectors. Not many want to be tracked by the authorities, or treated like human bar code. Myriad benefits will accrue from the further deployment of identification techniques—even personally identifiable—into various facets of daily life. But where is the line crossed, and who is capable of crossing it?

In private hands, techniques like behavioral marketing, biometric and data-mining technologies enlarge our horizons. They expand the possibilities of a market economy by bolstering security in private transactions ranging from face-to-face authentication to long-distance commerce. The best, most secure technologies are those that *prevent others from posing as us*—that's why the value of personally identifiable data cannot be ruled out. The Web is desperately short of that kind of clarity and authentication, in a world of cyber-risks, identity theft, and the need to conduct ever more sensitive transactions. But nothing is automatic. The marketplace imperative requires private sector experimentation in privacy: It's messy, but necessary.

On the one hand, policy should not create situations where companies are required to ask for personal info that otherwise wouldn't be needed. (Google declares in its comments on the FTC advertising principles that obeying certain rules would require it to collect information it otherwise would not need.) On the other hand, certain forms of identifiable behavioral tracking may prove important in specific contexts and shouldn't be prohibited.

Disallowing personally identifiable information nis the wrong thing to do. We often need to identify those we're dealing with on line, and for them to be able to identify us; such instruments will be governed by heretofore unknown contracts and privacy polices. It's not "self-regulation," but the needs of the world at large driving this evolution. Rather than legislating, it's likely better to keep this a war between computer scientists; between those working on behavioral advertising with personal information and/or authentication, and those working on behavioral without authentication. Being able to sell to a customer but not have that customer identified is a key research area in computer science. The consumer-control ethos—the notion that we don't have to be tracked—puts consumers, not advertisers, in the drivers' seat Let the computer scientists duke it out.

In many transactions and contexts, the Web needs better authentication, not the abandonment of personally identifiable information. The private sector should experiment with generating such data in ways that consumers can accept. Some say we must regulate because online risks exist; this report argues for *not* regulating because there are online risks. The firms that reduce risks in ways palatable to consumers offer a great service. New products and institutions still need to emerge around online commerce.

Expanding the Marketplace for Liability and Private Security Insurance

Privacy is one subset of the much broader issues of online security and cybersecurity. It's been noted that a basic problem today is that no one stands in any position to make guarantees to anybody about anything. That doesn't mean improved insurance products and enhanced liability contracts won't develop online, however. Lessons learned from spam, privacy, and preventing piracy of intellectual property will carry over to the security issues of tomorrow.

Government shouldn't grant immunity to software companies for breaches, but at the same time it should not impose liability on them either. It's not so clear whom to sue on an Internet not amenable to authentication, but standards will emerge. Government interference can impede private cyber-insurance innovations

Certain innovations can be sacrificed by regulating. The private sector needs to "practice" now for the really difficult cases like the integration of biometrics into the online world; meanwhile the federal government needs to focus on cyber-crime.

A Positive Agenda for the Federal Government

Policymakers should appreciate the government's inherent limitations as well as the vulnerabilities that can be created by federal policies and procedures.

From lost laptops to hacks into the Pentagon email system, to "D" grades for the Department of Homeland Security's own information security practices, regulators' ability to rationally guide others on privacy is questionable. In many areas it makes sense to circumscribe regulators' sphere of influence, while increasing that of the market.

Recognizing that governments can fail just as markets can, there are numerous ways government within its limitations can *properly* foster private sector innovation in security:

- Foster competitive discipline
- Emphasize protecting government's own insecure networks, not regulating markets. This means many things, including: removing sensitive information from government websites; limit the size and scope of government databases to ensure government doesn't create artificial cybersecurity risks; avoiding data retention

mandates and other interventions that undermine private-sector security guarantees.
- Focus on computer criminals, not cyber-regulations
- Assess areas where it's best to *liberalize* private sector data-sharing rules. For example, facilitating private sector medical data sharing could deliver benefits to suffering patients. More broadly, some firms cannot share data among their own divisions because of antitrust and privacy strictures. Enhancing cross-firm coordination can improve reliability and security
- Recognize that commercial anonymity and political anonymity differ; we may need "less" of the former, even as we expand the latter. Research should continue on the seemingly opposed agendas of authentication of users on the one hand, and anonymizing technologies on the other.

Conclusion: Affirming Private Sector Primacy Over Information Practices.

Our greatest privacy concern should be government collection of our information, not the emergence of targeted marketing.

In the changing world of e-commerce, the role of government is not to predetermine commercial privacy arrangements, but to enforce information-sharing contracts that companies make between themselves or with individuals. Privacy policies are legally binding. Government's role is not to dictate the structure of privacy contracts through such means as opt-in or opt-out policies; it is to halt deceptive practices and hold private firms accountable to the guarantees they make. Government's other role is to protect citizens from identity theft, which is not a commercial enterprise, but a criminal one.

If anonymity and the inability to exclude bad actors are at the root of genuine online security problems, legislation doesn't make them go away. When contemplating centralized government vs. decentralized market approaches to protection consumers onlie, we must strive, before regulating, to follow the "cybersecurity commandment": *Don't entrench regulation to such a degree that effective private alternatives and institutions, however warranted as conditions change, simply cannot emerge*.

Appendix: Related Reading

Wayne Crews and Ryan Radia, "Rigid Federal Mandates Hinder Privacy Technologies," *San Jose Mercury News*, June 15, 2008, http://www.mercurynews.com/opinion/ci_9593341

Wayne Crews, "Cybersecurity Finger-pointing: Regulation vs. Markets for Software Liability, Information Security, and Insurance," CEI Issue Analysis 2005 No. 7, May 31, 2005, http://cei.org/pdf/4569.pdf.

Wayne Crews, "Cybersecurity and Authentication: The Marketplace Role in Rethinking Anonymity—Before Regulators Intervene," CEI Issue Analysis 2004 No.2, November 8, 2004, http://cei.org/pdf/4281.pdf.

Wayne Crews, Comments to the FTC on email authentication themes, September 30, 2004, http://www.cei.org/pdf/4229.pdf.

Alberto Mingardi and Wayne Crews, EU takes a Swipe at Google, *International Herald Tribune*, March 9, 2007, http://www.iht.com/articles/2007/03/09/opinion/edmingardi.php.

Wayne Crews and Brooke Oberwetter, "Preventing Identity Theft and Data Security Breaches: The Problem With Regulation, CEI Issue Analysis 2006 No. 2, May 9, 2006, http://cei.org/pdf/5316.pdf.

Wayne Crews "Giving Chase in Cyberspace: Does Vigilantism Against Hackers and File-sharers Make Sense?" CEI OnPoint No. 109, October 2, 2006. http://cei.org/pdf/5569.pdf.

Wayne Crews, "Trespass in Cyberspace: Whose Ether Is It Anyway?" TechKnowledge #19, Cato Institute, September 10, 2001, http://www.cato.org/tech/tk/010910-tk.html.

Wayne Crews, "Human Bar Code: Monitoring Biometrics Technologies In a Free Society," Cato Institute Policy Analysis No. 452, September 17, 2002, http://www.cato.org/pubs/pas/pa452.pdf.