J Consum Policy (2008) 31:473–487
DOI 10.1007/s10603-008-9082-5

ORIGINAL PAPER

When Should "Consumers-as-Producers" Have to Comply With Consumer Protection Laws?

Peter P. Swire

Received: 6 July 2008 / Accepted: 13 October 2008 /
Published online: 14 November 2008

Abstract Since the 1960s, consumer protection law has been built on the contrast between large "producers" and small "consumers." Today, instead, an ordinary consumer owns what can accurately be called a "personal mainframe"—a home computer whose processing power matches an IBM mainframe from about 10 Years ago. Equipped with a personal mainframe—an Information-Age factory—ordinary "consumers" at home are increasingly also becoming "producers." As unregulated consumers become regulated producers, a major legal question is whether and when the individual should have to comply with consumer protection laws. The discussion here selects four examples of US legal rules that might apply to consumers-as-producers, with recommendations spanning the range of possibilities: (1) consumer privacy legislation: creating a threshold, with no compliance required for databases of fewer than 5,000 names, is recommended; (2) advertising substantiation: concerning the requirement that advertisers have a "reasonable basis" for their claims, applying current law to small advertisers is recommended; (3) spam: current law does not create a threshold for those who send a few commercial emails, but such a threshold is worth considering; (4) political blogging: the author agrees with the US Federal Election Commission decision to create a major exemption from campaign finance laws for online political advocacy, even for large blogs or websites. The common theme among these recommendations is to describe the sort of harm that existing law seeks to reduce. The approach here next looks at how the use of personal mainframes affects creation of those harms. Where the sorts of harm are likely to be created by consumers-as-producers, the analysis tilts towards requiring compliance. Where the sorts of harms are unlikely to be caused by consumers-as-producers, then the case for an exception is stronger.

P. P. Swire
Moritz College of Law, Ohio State University, Columbus, OH, USA

P. P. Swire (✉)
8520 Howell Road, Bethesda, MD 20817, USA
e-mail: peter@peterswire.net

P. P. Swire
Center for American Progress, Washington, DC, USA

Keywords Consumer protection · Cyberlaw · Electronic commerce · Advertising · Data protection

This article emerges from a larger research project on how computers and the Internet change consumer protection.[1] Since the 1960s, consumer protection law has been built on the contrast between large "producers" and small "consumers." Today, instead, an ordinary consumer owns what can accurately be called a "personal mainframe"—a home computer whose processing power matches an IBM mainframe from about 10 Years ago. Equipped with a personal mainframe—an Information-Age factory—ordinary "consumers" at home are increasingly also becoming "producers."

As unregulated consumers become regulated producers, a major legal question is whether and when the individual should have to comply with consumer protection laws. There are three logical possibilities:

1. Individuals should be regulated as producers.
2. Producers should no longer be regulated.
3. A threshold should be defined, below which small producers are not regulated.

The legal and analytic problem exists because both labels are essentially correct. The individual is now acting as a "producer." As such, the individual might now perpetrate the sort of harm that led to the consumer protection law in the first instance. For instance, individuals who sell goods might engage in fraud or deceptive practices. Perhaps consumer protection laws should thus apply in full measure to consumers-as-producers.

On the other hand, the individual is still a "consumer." Simply by using personal mainframes to engage in some commercial activity, individuals do not become sophisticated, experienced, and able to avoid the cognitive biases that consumers often show.[2] Individuals also face potentially significant barriers to compliance with consumer protection laws. They often will not know what is required by law, and the scale of their commercial activity will not justify expensive legal counsel. Perhaps consumers-as-producers should thus be exempt from having to comply with consumer protection laws.

The discussion here selects four examples of US legal rules that might apply to consumers-as-producers, with recommendations spanning the range of possibilities:

1. Consumer privacy legislation: creating a threshold, with no compliance required for databases of fewer than 5,000 names, is recommended.
2. Advertising substantiation: Concerning the requirement that advertisers have a "reasonable basis" for their claims, applying current law to small advertisers is recommended.
3. Spam: current law does not create a threshold for those who send a few commercial emails, but such a threshold is worth considering.
4. Political blogging: the author agrees with the US Federal Election Commission decision to create a major exemption from campaign finance laws for online political advocacy, even for large blogs or websites.

The common theme among these recommendations is to describe the sort of harm that existing law seeks to reduce. The approach here next looks at how the use of personal mainframes affects creation of those harms. Where the sorts of harm are likely to be created

[1] Swire (1998, 2003, 2005, 2006, 2008). See also National Consumers League (2006). The author served as "reporter" for that document.

[2] For a discussion of such cognitive biases, see Garvin (2005).

by consumers-as-producers, the analysis tilts towards requiring compliance. Where the sorts of harms are unlikely to be caused by consumers-as-producers, then the case for an exception is stronger.

Consumer Privacy Legislation

Congress is beginning to pay more attention again to the topic of consumer privacy legislation to apply to on-line commerce but also likely to off-line. The author testified in a hearing on the subject in 2006,[3] and major industry players have now called for a national law.[4] A group of companies has specifically stated:

> In principle, such legislation would address businesses collecting personal information from consumers in a transparent manner with appropriate notice; providing consumers with meaningful choice regarding the use and disclosure of that information; allowing consumers reasonable access to personal information they have provided; and protecting such information from misuse or unauthorized access. Because a national standard would preempt state laws, a robust framework is warranted.[5]

The author has written elsewhere about why he thinks such legislation was premature when proposed during the 1990s but why the case for legislation is considerably stronger today.[6]

The author's support for legislation, however, has long been beset by a specific doubt. The author has not known how to define the threshold for when such legislation might apply. The problem is illustrated by the example of the author's teenage son, who made money one recent summer by cutting the lawns for perhaps eight neighbors. Suppose his son wanted to tell the neighbors' names to a friend, who was planning to cut lawns the following summer. Should his son be required to have given prior written notice to each family, with an opt-out box for neighbors who did not want their names shared? In the terms of this article, when the author's son acts as a "producer"—a lawn-cutting enterprise—should he have to comply with this consumer protection law?

From having discussed this example in various settings, the clear answer is no. One reason is that the degree of privacy harm is de minimis—the reasons supporting a privacy regime do not apply well to this casual activity of neighbors.[7] Another reason is political. If

[3] Hearing on "Privacy in the Commercial World II" Before the Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce, 109 Cong. 30 (2006) [hereinafter *Hearings*] (testimony of Peter P. Swire, William O'Neill Professor of Law, Moritz College of Law).

[4] Id.

[5] Id.

[6] Swire (2003) pp 859–871. In brief, self-regulation in the 1990s speeded the adoption of good practices by most E-Commerce sites. The credible threat of legislation during that period pushed industry to make relatively rapid progress. Once the threat of legislation receded, however, the pace of improvement slowed. In addition, lessons learned from other privacy laws passed in the 1990s now form a solid foundation for workable general privacy legislation.

[7] The author has explained previously reasons why the degree of privacy invasion is much greater for large databases than for the sorts of small, unaggregated "databases" that the teenage lawn-cutter would create. Swire (2005).

a US privacy law purported to regulate the lawn-cutters and baby-sitters of America, it would never be enacted. If it were enacted, it would soon be repealed.[8]

Nor is the solution under the European Union Data Protection Directive very attractive. The Directive does have an exemption for non-commercial activities "by a natural person in the course of a purely personal or household activity."[9] Cutting a lawn for money, however, is not "purely personal." The teenager, based on the text of the law, is supposed to comply with the full set of data protection rules. The European response has been that officials would use discretion in enforcement (Swire and Litan 1998). In this approach, the teenager can ignore the law, believing that no enforcement will occur.

As has been discussed before, however, this sort of illegal-but-not-enforced approach is undesirable and a bad fit with American legal practice (Swire and Litan 1998). Overbroad legislation, to the extent it generates compliance, leads to needless costs and burdens on the teenager and all others who should not be included. Overbroad legislation fails to provide clear notice of what is prohibited and creates the risk of arbitrary and discriminatory enforcement. American lawyers and companies are reluctant to break the law knowingly, given potentially significant legal sanctions if they do.[10] In addition, a perception that legislation is unenforceable can make the law a dead letter. The achievable good purposes of legislation can be lost if the law purports to go too far.

A good answer has recently emerged, however. A small producer exception can apply based on the number of persons whose data are used by the producer. One proposal would be to exempt an entity that "collects, stores, uses or discloses personal information from fewer than 5,000 individuals" in a 12-month period.[11] For smaller collections of data, the benefits of privacy protection are outweighed by the burdens of compliance by the lawn-cutters of America. For larger collections of data, which usually are maintained in well-known software formats, compliance with the privacy requirements can be integrated with the software. For employment law, the small-producer exemption has long been based on

[8] An example of speedy repeal was a strict medical privacy law in Maine that prevented flowers from being delivered to patients in the hospital. The problem for florists was that they needed prior patient consent to learn the number of the hospital room, but the patients were usually receiving the flowers as a gift and so had not given prior consent. See Goldstein (1999).

[9] Council Directive 95/46 art. 3 EC OJ [1995] L281/31.

[10] Swire and Litan (1998). Under the US Sentencing Guidelines, an upward departure may be appropriate when a corporation has demonstrated a pattern of illegal conducts. US Sentencing Guidelines Manual §8C2.8 comment. n. 5 (2005). Under Sarbanes-Oxley, there is heightened pressure for public companies to have accurate and lawful systems in place. See, e.g., 15 U.S.C. §7241(a) (2007) (requiring corporate officers to personally certify financial reports based upon the officer's own knowledge).

[11] The first public mention of this approach was apparently in the testimony of Microsoft Senior Attorney Michael Hintze before the House Energy & Commerce. *Data Security: The Discussion Draft of Data Protection Legislation* before the Subcommittee On Commerce, Trade, and Consumer Protection, 108th Congress (2005): http://www.microsoft.com/presspass/exec/hintze/07-28-05DataSecurity.mspx (statement of Michael Hintze, Senior Attorney, Microsoft Corporation).

The 5,000-individual approach was suggested in connection with proposed federal legislation to require producers to notify consumers in the event of a data breach. The concerns about a threshold for data breach legislation are very similar to those for privacy legislation. For instance, if a friend loses a PDA, laptop, or other device holding contacts information, should that person be legally required to send you formal written notice of the loss? It may be polite to do so (if the friend has a kept a backup and so knows whom to contact). The author's own sense is that it would be overbroad to require individuals that have a modest number of business contacts to be covered by federal legislation. A data breach bill with a threshold of 10,000 individuals has been passed by the Senate Judiciary Committee. S. 495 § 301, 110th Congress, First Session.

the number of employees.[12] When it comes to data about individuals, the exemption can be based on the number of individuals in the database.

Advertising by Small Producers

Various laws apply to producers in the USA when they advertise. To take two examples, consumer protection laws now impose rules on direct marketers who telephone, fax, or send e-mail to the home.[13] Commercial advertisers are also subject to various anti-fraud rules, such as the requirement that they substantiate claims contained in their advertisements. The question for our purposes is the extent to which these advertising rules should apply to individuals as they shift into also becoming producers.

Advertising Substantiation

Suppose a company makes a claim in a television advertisement: "Diapers by X keep a baby dryer than diapers made by Y." Under long-standing law, the claim must be "substantiated," or else, it will be considered a deceptive trade practice. What if the text of a blog says the same thing? The typical blogger does not do a careful empirical study before typing his or her opinion and sending it off to the blogosphere. Advertisements are now shifting from broadcast to narrowcast, increasing the number and range of advertisements. The cost of producing many types of advertisements also has plummeted, as personal mainframes bring non-embarrassing production values within the realm of the individual user. The question is how much of the regulatory overhead from the broadcast, large-scale production era should apply to consumers-as-producers.

The "FTC Policy Statement Regarding Advertising Substantiation" was issued in 1984 and remains in force today.[14] The Statement announces the basic legal rule, "that advertisers and ad agencies have a reasonable basis for advertising claims before they are disseminated."[15] For those unfamiliar with advertising law, it may be surprising that the substantiation must exist in advance: "[A] firm's failure to possess and rely upon a reasonable basis for objective claims constitutes an unfair and deceptive practice in violation of Section 5 of the Federal Trade Commission Act."[16] For claims made in an advertisement, "advertisers will not be allowed to create entirely new substantiation simply because their prior substantiation was inadequate."[17] The author has not found previous discussion of the extent to which the substantiation requirement applies to consumer-

[12] Title VII of the Civil Rights Act defines "employer" as "a person engaged in an industry affecting commerce who has fifteen or more employees for each working day in each of twenty or more calendar weeks in the current or preceding calendar year, and any agent of such a person." 42 U.S.C. §2000(e) (2007). Similarly, the Age Discrimination in Employment Act sets the threshold at twenty employees. 29 U.S.C. §630 (b) (2007).

[13] The Do Not Call registry does not have an exception for small business. Telemarketing Sales Rule, 16 C.F.R. §310.4 (b)(1)(iii)(B) (2007). The Junk Fax Prevention Act of 2005, 47 U.S.C.S. §227(b)(2)(D)(iv)(II), authorized the Federal Communications Commission to create a small-business exception. Based on its finding that compliance would not be burdensome for small businesses, the Federal Communications Commission declined to create such an exception. *Federal Register, 71*, 29,577 (May 3, 2006).

[14] FTC Policy Statement Regarding Advertising Substantiation: www.ftc.gov/bcp/guides/ad3subst.htm.

[15] Id.

[16] Id., citing to 15 U.S.C. § 5.

[17] Id.

produced content. The discussion here of substantiation law, moreover, illustrates the analysis that might apply to consumers-as-producers for other advertising laws, such as truth-in-labeling with respect to third-party endorsements,[18] or guidance concerning word-of-mouth advertising.[19]

The substantiation requirements have applied most clearly to advertisements produced on an industrial scale, especially national advertisements on television.[20] The Federal Trade Commission (FTC) has long recognized, however, that small businesses also advertise. Its guidance shows that even small businesses must comply with potentially significant requirements:

> Before a company runs an ad, it has to have a "reasonable basis" for the claims. A "reasonable basis" means objective evidence that supports a claim. At a minimum, an advertiser must have the level of evidence that it *says* it has. For example, the statement "Two out of three doctors recommend ABC Pain Reliever" must be supported by a reliable survey to that effect. If the ad isn't specific, the FTC looks at several factors to determine what level of proof is necessary, including what experts in the field think is needed to support the claim. In most cases, ads that make health or safety claims must be supported by "competent and reliable *scientific* evidence"—tests, studies, or other scientific evidence that has been evaluated by people qualified to review it. In addition, any tests or studies must be conducted using methods that experts in the field accept as accurate.[21]

Advertising rules apply not only to small businesses but also to online businesses. The FTC has announced that "[t]he same consumer protection laws that apply to commercial activities in other media apply online" (Federal Trade Commission 2000a). The need for substantiation specifically applies online (Federal Trade Commission 2000b).

The author tentatively believes that it makes sense to retain the substantiation and similar advertising rules for consumers-as-producers. Suppose the home-based web site advertises that "studies show that our herbal home remedy dramatically improves your chances of surviving breast cancer." This type of health claim has been a frequent target of false advertising enforcement.[22] Although sophisticated readers of law reviews might not fall for such a pitch, bitter experience shows that patients often pay large amounts in their desperate search for a cure.

We can generalize from the false health claim example. In speaking with experts who have litigated advertising cases,[23] a consistent theme was that fraud often happens in one-on-one settings. Making an unsupported and deceptive claim, to even one consumer, can

---

[18] Federal Trade Commission, *Guides Concerning Use of Endorsements and Testimonials in Advertising*, 16 C.F.R. Part 255.

[19] A 2006 speech by an FTC official said that the Endorsement Guidelines apply to word-of-mouth advertising. In particular, word-of-mouth advertisers should disclose "a connection between a seller and an endorser that might materially affect the weight or credibility of the endorsement." Engle (2006); see Carl (2006).

[20] "The FTC concentrates on national advertising and usually refers local matters to state, county, or city agencies." Federal Trade Commission. *Advertising Practices: Frequently Asked Questions. Answers for Small Business*, 7: http://www.ftc.gov/bcp/conline/pubs/buspubs/ad-faqs.pdf.

[21] Id. at 5 (emphasis in the original).

[22] "The FTC concentrates on cases that could affect consumers' health or safety (for example, deceptive health claims for foods or over-the-counter drugs)." Federal Trade Commission, supra note 19.

[23] E.g., interview with Diana Bixler, former FTC attorney, Jan. 30, 2007.

readily harm that consumer. The very basis for the regulation—protection against fraud—thus counsels for applying the regulation to individual instances of harm. Even a very small producer should likely be covered.[24]

Controlling the Assault of Non-Solicited Pornography and Marketing

Advertising also happens directly from one seller to one consumer. The problem of "spam"—unsolicited commercial email—has expanded as the Internet has expanded. In 2003, Congress passed the "Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM)" Act in an attempt to protect consumers from these unwanted emails.[25] CAN-SPAM has been a colossal failure at achieving the goal of eliminating all unwanted email. The author suggests, however, that the law has more-or-less succeeded at meeting a different goal—establishing basic standards for how an individual can stop receiving email from legitimate companies. The question here is the extent to which CAN-SPAM should also apply to consumers-as-producers.

For ordinary businesses, the main requirements of CAN-SPAM are that the business be easy to contact and that it stop sending commercial emails once the consumer asks. The email must include the physical postal address of the sender and must have a functioning return email address or other Internet-based mechanism for contact by the consumer.[26] The contact information must stay valid for at least 30 days, so the consumer can readily opt out of receiving future emails.[27] The scope of coverage is traditional for consumer statutes, applying to "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service."[28] For the criminal fraud provision, there are some thresholds for greater penalties based on the number of false email accounts and the number of fraudulent emails sent.[29]

The spam problem today is really two quite distinct consumer protection problems. The first problem comes mostly from black-market rings of spam producers, mostly located outside of the USA. These spam rings constantly change their technology to evade anti-spam measures. The author has learned, from working as an advisor to a company that sought to shut down these spam rings, that this black-market spam is created by organized

[24] One alternative would be to create an exception so that small businesses do not need to create studies or other prior substantiation. Under this approach, for small companies, there could be a "reasonable basis" for a claim if there is a good-faith belief in its truthfulness. Under such an approach, the intentional swindler could still be punished. The false claim about breast cancer, for instance, might be punished under a criminal fraud statute or under civil statutes if there is a reckless or intentional misstatement. This alternative would free the consumer-as-producer from the need to substantiate in advance the "reasonable basis" for the claim. The alternative approach, however, would create an enforcement challenge because enforcement agencies would then have to prove a heightened mens rea in the case of an unsubstantiated advertisement.

[25] Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM), 15 U.S.C. §7701 et seq.

[26] CAN-SPAM, supra note 25. § 5.

[27] CAN-SPAM, supra note 25. § 5.

[28] CAN-SPAM, supra note 25. § 3(2), 15 U.S.C. § 7702.

[29] CAN-SPAM, supra note 25. § 4(a), 15 U.S.C. § 7703.

crime groups that operate primarily outside of the USA including in Eastern Europe.[30] As the author has written previously, the law does not operate effectively against "mice" that use the Internet from nests offshore,[31] even the somewhat larger criminal rings that now send most of the black-market spam.[32]

CAN-SPAM has a much more significant effect on how legitimate businesses send email to consumers. If you buy a computer, then you might expect or even welcome emails from the manufacturer telling you about updates or accessories. If you join a music club, then you get emails about upcoming concerts or music releases. What CAN-SPAM does, pretty successfully, is to give legitimate businesses a minimum standard for sending commercial emails to individuals.[33] Once you decide not to receive the computer or music club emails any more, you can unsubscribe. Those emails will then typically stop.[34]

How should CAN-SPAM apply to consumers-as-producers? For instance, suppose a blogger sends email to five commenters to the blog, asking if they would like to gain the privilege to post blog entries for a fee of $20/month. The statute is triggered if the "primary purpose" of the email is commercial advertisement or promotion. On its face, the email quite possibly seems commercial—it asks for money in exchange for something the five recipients might value. In practice, there may a different primary purpose for the email, such as sharing costs to run a political blog. In short, detailed facts about the sender and the five recipients may shift our conclusion about whether the statute applies.

Although the statute does not currently have an exception for consumers-as-producers, such an exception may be appropriate. To take a simple example, suppose you send an email to a long-lost friend from high school, whom you have not seen in years, seeing if the friend wants to buy something you have made or a service that you offer. In order to send

[30] In 2005 and 2006, the author served on an advisory board to Blue Security. The company had innovative software that enabled each user to send one opt-out message to the web site selling the product advertised in the spam email (that is, the software made it easy for the user to exercise the opt-out right in CAN-SPAM). The volume of legitimate opt-outs created large traffic on the web sites. To reduce this traffic, the web sites could receive a free, encrypted do-not-spam service from Blue Security. This approach was succeeding—six of the ten largest spammers in the world began using the do-not-spam service.

Unfortunately, one of the remaining spammers declared war on Blue Security. In classic organized-crime fashion, the person or group labeled "PharmaMaster" lashed out at everyone connected with Blue Security. Denial-of-service attacks ultimately affected hundreds of thousands of web sites. Krebs (2006). Singel (2006).

Based on this experience, the author concludes that the problem of black-market spam cannot be solved by passing a law or regulation. Effective action will require the sorts of efforts that have been used against the Mafia or other organized crime rings. Notably, the organized crime rings must be denied safe havens where they are protected by local authorities while retaining open access to the Internet.

[31] At the end of 2006, the Federal Trade Commission gained some much-needed powers to cooperate with international authorities, in order to enforce against cross-border fraud. US SAFE WEB Act of 2006, Pub. L. No. 109–455, 120 Stat. 3372.

[32] In earlier writings, that author has argued that law works relatively well on the Internet to regulate "elephants," which are larger organizations, but much less well against "mice," which breed quickly on-line and often hide offshore. See Swire (1998, 2005). One new development is the increased scale of black-market Internet operations. Small spam operations cannot keep up with new technology. The result is that most black-market spam today is sent by what Ari Schwartz has quipped are "rodents of unusual size." Physorg.com (2006).

[33] The chief problem in practice is that it can be difficult for consumers to be certain that the address provided for opt-out is legitimate and not a fake site used by fraudsters. For ways to address this phishing problem, see National Consumers League (2006).

[34] If the emails do not stop, then enforcement against a legitimate business is relatively easy. The consumer can easily save a copy of the opt-out request and a copy of the continued commercial emails. Although there is no private right of action for consumers, this sort of evidence forms an easy case for state attorneys general and others authorized under the statute to sue.

that email, should you be required to include your postal address (which you might not want to share) and maintain a Web presence for at least 30 days? Should you have to consult an attorney to see whether your email triggers the CAN-SPAM requirements?

In the face of these compliance requirements on millions of consumers-as-producers, it may be possible to craft a threshold, such as a dozen or 50 commercial emails per day.[35] A threshold of that sort might enable individualized emails that are primarily commercial, while maintaining the usual CAN-SPAM requirements on mailings of significant size.[36] The CAN-SPAM prohibitions on false email headers could apply even to consumers-as-producers.[37] In that way, the recipient would have a fairly easy way to identify and contact the sender to opt out of future contacts. Perhaps the FTC or Congress could hold hearings to determine how well such a threshold would work in practice.

The Federal Election Commission and Blogging: When Do Favorable Comments Become "Campaign Contributions"?

The campaign finance laws impose complex regulations on large media such as newspapers and television stations. There are rules, for instance, that govern when free advertisements or other activities by the media company count as regulated "contributions" to a political campaign.[38] Under the McCain–Feingold reforms of 2002, to take another example, political advertisements require a disclaimer along the lines of "this advertisement was paid by the campaign to re-elect Senator X."[39] An important question, which erupted into a major debate in 2005 and 2006, is how these campaign finance rules apply to that vocal species of consumer-as-producer, the political blogger.

The Federal Election Commission ("FEC") was required by a court decision to clarify how the campaign finance laws applied to the Internet. McCain–Feingold provided that key political players use only "Federal" funds—the hardest funds to raise—for any "public communication" that promotes, supports, attacks, or opposes a clearly identified candidate for Federal office.[40] Congress defined "public communication" in a way that listed traditional media such as television and newspapers but failed to mention the Internet.[41] The initial FEC rules explicitly

[35] In a somewhat analogous context, discussed directly below, the Federal Election Commission in 2006 created a threshold of 500 substantially similar emails for when certain campaign-finance disclaimers are required. *Federal Register, 71*, 18,589 (Apr. 12, 2006).

In discussions on background with some attorneys with enforcement experience, concern was expressed that it may be burdensome to require enforcers to show more likely than not that only a small number of emails had been sent. To address this practical enforcement concern, it could perhaps be an affirmative defense that the sender was sending only a small number of emails.

[36] The harm to individual recipients is also likely to be negligible—the problem of a flooded in-box does not result from occasional, individualized emails.

[37] 15 U.S.C. §7704 (a)(1).

[38] Under the FEC's longstanding media rules, news stories, commentaries, and editorials (including endorsements) are exempt from regulation unless the media facility is owned or controlled by a candidate, political party of FEC-registered political committee. 11 C.F.R. § 100.73 & .132. By contrast, free or below-market advertisements provided by media facilities are considered political contributions.

[39] Bipartisan Campaign Reform Act of 2001, Pub. L. 107-155, 116 Stat. 81 (2002), amending the Federal Election Campaign Act of 1971, as amended, 2 U.S.C. § 431 et seq.

[40] The limits applied to State, district, and local political party committees and organizations, as well as State and local candidates. See Internet Communications (2006).

"Federal" funds are funds subject to the limitations, prohibitions, and reporting requirements of federal campaign finance laws. See 11 C.F.R. § 300.2(g).

[41] 2 U.S.C. § 431(22).

excluded all Internet communications from the definition of "public communication,"[42] but this interpretation was struck down in federal court.[43]

The FEC was thus obliged to revise its rules in response to the court decision. The political blogging community suddenly became aware that it might become subject to complex campaign finance regulations, as well as FEC fines and other enforcement actions. After all, bloggers incessantly "promote, support, attack, or oppose" clearly identified candidates for political office. If the FEC decided to be expansive in the scope of its Internet regulation, then there could have been profound effects on the way that bloggers engaged in political advocacy.

Any student of interest-group politics would not be surprised by the next episode in the drama—political bloggers on the left and right united in opposition to being regulated.[44] As will be explained, however, in this instance, the author believes the opposition was entirely correct. The FEC eventually agreed, and the revised rules place a light touch on the Internet. The definition of "public communication" continues to exclude communications over the Internet, except for paid advertisements placed on another person's website.[45] Uncompensated blogging, whether done by an individual or a group of individuals, is exempt from regulation.[46] In addition, regardless of the content that appears on an individual's or a group's website, a disclaimer is not required unless the individual or group is a registered political committee.[47] In summary, the final rules "make plain that the vast majority of Internet communications are, and will remain, free from campaign finance regulation."[48]

For supporters of campaign finance, this victory for the bloggers may seem like a defeat for efforts to achieve the goals of campaign finance. Two responses would be highlighted of the longer list generated by the bloggers and their allies. The first concerns the constitutional protection of free speech, which has shaped the entire field of campaign finance law since *Buckley v. Valeo* in 1975.[49] If consumers-as-producers are treated like traditional producers (such as television stations), then the number of entities subject to complex campaign finance rules would rise by orders of magnitude. In light of the numerous previous laws that have been struck down on First Amendment grounds,[50] it was likely prudent for the FEC to be cautious in so greatly expanding the reach of its rules.

[42] 11 C.F.R. 100.26; Final Rules on Prohibited and Excessive Contributions; Non-Federal Funds or Soft Money, *Federal Register, 61*, 49,064 (July 29, 2002).

[43] *Shays v. Federal Election Comm'n*, 337 F.Supp. 2d 28 (D.D.C. 2004), aff'd, 414 F.3d 76 (D.C. Cir. 2005).

[44] See, e.g., Center for Democracy & Technology and Institute, for Politics, Democracy & the Internet (2005).

[45] 11 C.F.R. § 100.26. FEC Commissioners Lenhard and Weintraub issued a quite readable summary of the revised regulation. Lenhard and Weintraub (2006).

[46] 11 C.F.R. § 100.94 & .155.

[47] 11 C.F.R. § 110.11.

[48] *Federal Register, 71*, 18,590. The intent of the FEC is clear: "To the greatest extent permitted by Congress and the *Shays District* decision, the Commission is clarifying and affirming that Internet activities by individuals and groups of individuals face almost no regulatory burdens under the Federal Election Campaign Act." Id.

[49] *Buckley v. Valeo*, 424 U.S. 1 (1975).

[50] E.g., *Randall v. Sorrell*, 126 S. Ct. 2479, 2485 (2006) (plurality opinion) (finding a Vermont campaign finance statute's expenditure and contribution limitations in violation of the First Amendment); *Fed. Election Comm'n v. Mass. Citizens for Life*, 479 U.S. 238, 241 (1986) (holding unconstitutional a provision of the Federal Election Campaign Act limiting corporate expenditures "in connection with" federal elections); *First Nat'l Bank v. Bellotti*, 435 U.S. 765, 767 (1978) (finding unconstitutional on First Amendment grounds a Massachusetts statute limiting corporate contributions and expenditures designed to influence voters).

Second, and more profoundly, the FEC appreciated that robust political speech on the Internet actually *furthers* the goals of the regulatory regime instead of being a loophole. Without using the term, the FEC recognizes the importance of consumers-as-producers: "[I]ndividuals can create their own political commentary and actively engage in political debate, rather than just read the views of others."[51] The ability of millions of people to produce and disseminate political views contrasts with traditional media: "Unlike television, radio, newspapers, magazines, or even billboards, the Internet can hardly be considered a scarce expressive commodity. It provides relatively unlimited capacity for communication of all kinds."[52]

Principal rationales for campaign finance rules are to reduce corruption in politics and to prevent monopolization of political discourse.[53] The low cost of Internet communications and the enormous numbers of new political speakers who are facilitated by the Internet mean that greater political speech on the Internet advances both rationales. The corrupting influence of money is less when effective political communication is possible for ordinary consumers-as-producers.[54] Monopolization of discourse is also avoided: "The Internet's user-driven control and decentralized architecture support a multiplicity of voices and constrain the ability of any one speaker to monopolize attention or drown out other voices."[55]

Generally exempting Internet speech from campaign finance laws thus furthers the goals of such laws. Conversely, strict application of campaign finance laws to the Internet would undermine the laws' goals. If political statements on a blog require compliance with complex campaign finance rules, then the costs of blogging rise substantially. With higher cost comes a lower supply of speech. To put the point in familiar First Amendment language, there would be a major "chilling effect."

Looking ahead, there have already been proposals to bring large Internet sites into the campaign finance regime.[56] Such proposals likely should be rejected. As already explained, the architecture of Internet speech differs from broadcast speech—there is not the same scarcity and risk of monopolization. In addition, many popular political sites on the Internet are not primarily commercial in the way that newspapers and television stations are

[51] *Federal Register, 71*, at 18,590.

[52] Id, quoting *Reno v. ACLU*, 521 U.S. 844, 970 (1997) (internal quotations omitted).

[53] The prevention of corruption was identified in *Buckley* as the principal governmental interest that justified limits on campaign contributions. *Buckley v. Valeo*, 424 U.S. at 31. As stated in the Joint Principles: "Robust political activity by ordinary citizens on the Internet, including their monetary contributions, strengthens and supports the central underlying purpose of the campaign finance law: to protect the integrity of our system of representative democracy by minimizing the corrupting influence of large contributions on candidates and office holders." Joint Principles, supra n. 44, at 2. The risk of monopolization of political discourse, due to the scarcity of traditional broadcast media, has formed the basis for the Fairness Doctrine and other regulation of traditional media. *Red Lion Broadcasting Co. v. FCC*, 395 U.S. 367 (1969).

[54] The FEC stated: "Unlike other forms of mass communication, the Internet has minimal barriers to entry, including its low cost and widespread accessibility…[T]he vast majority of the general public who choose to communicate through the Internet can afford to do so." *Federal Register, 71*, 18,589–18,590.

[55] Joint Statement of Principles, supra n. 44, at 1.

[56] See Broache (2007).

commercial. For these largely non-commercial activities, which are created for political speech, the burden of compliance is not appropriate.[57]

Lessons for When "Consumers" Should be Regulated as "Producers"

The concept of consumer-as-producer proves helpful in analyzing the extent to which diverse regulatory regimes should apply to individuals who are equipped with personal mainframes. The unifying approach is to identify the harms that the regulatory regime is designed to address. For fraud in advertising, the harm can be created even by individual producers, and the existing regime should apply to small producers. For campaign finance on the Internet, by contrast, the new technological and market structure on the Internet mean that less regulation is actually likely better to achieve the goals of avoiding corruption and monopolization in political speech. For consumer privacy and anti-spam legislation, the harms are likely to be significantly greater for large producers. A threshold is thus appropriate, with regulation on large producers but not small ones.

Two other themes emerge from the analysis. First, we should be very hesitant to require millions of consumers-as-producers to do things that they would not otherwise do. For instance, the teenager who cuts lawns does not expect to print a privacy notice, and the sender of a personalized business email does not expect to include a postal address in each email. By contrast, ordinary individuals should have a "reasonable basis" for their claims when they advertise to sell products, such as in newspaper or online classified ads. Regulatory regimes more appropriately apply to consumers-as-producers the more that they track the standards of ordinary people acting in good faith.

Second, one should consider the likelihood that enforcement will be used to harass ordinary consumers-as-producers. One reason to exempt political bloggers from regulation is the high likelihood that complaints will be lodged by those holding different political views.[58] Ordinary political bloggers, therefore, would face the worry of having to hire a lawyer and respond to the complaint filed with the FEC. By contrast, the likelihood of harassing enforcement against a small advertiser seems relatively slight. A complaint is most likely to be lodged by a victim of fraud—someone who relied on the advertisement and was a disappointed consumer. For consumers-as-producers, the costs of defending an enforcement action may easily outweigh the commercial value of the enterprise. The

[57] In particular, the number of visitors to a site should not be the basis for triggering campaign finance requirements. An interesting political site may have no advertisements or other commercial activity at all. In addition, Internet sites sometimes attract huge bumps in visitors when they have newsworthy content. This dissemination of sought-after political news should not entail the penalty of having to comply with complex regulations.

If there is indeed movement over time to having some threshold, then a better threshold would likely be based on the scale of commercial activity. Proposed legislation in 2007 attempts to do this, but apparently, the definition of commercial activity is substantially overbroad. Major commercial sites are more analogous to the traditional entities subject to broadcast regulation. The presence of substantial commercial activities also means that the chilling effect will likely be less because funds will exist to hire lawyers and assure compliance.

[58] Joint Statement of Principles, supra n. 44.

different risk of over-enforcement thus supports having the advertising rule but not the campaign finance rules apply to consumers-as-producers.[59]

The methodology here is to assess the costs and benefits of consumer protection regulation, as applied both to large producers and producers-as-consumers. An ideal cost/benefit analysis would examine the following: (1) the costs and benefits of compliance by large producers; (2) the costs and benefits of compliance by consumers-as-producers; and (3) the costs and benefits of maintaining a threshold between large and small producers, if such a threshold exists.

This methodology assumes that many of the current consumer protection laws are worth having but that the laws should be thoughtfully updated with respect to consumers-as-producers. Other observers, such as Professor Richard Pierce, are more skeptical of the usefulness of such regulations. Professor Pierce disfavors many small business exceptions, arguing that fewer regulations would remain on the books if small businesses were subject to them and thus opposed them politically.[60] Although it would be Panglossian to believe that we are now in the best of all possible consumer protection worlds, the author is convinced enough by the economics and psychology literature about market failures that he believes the approach here is justified, to look at the harms addressed by each consumer protection law and focus on the extent to which consumers-as-producers are likely to contribute to those harms.

What is New About Today's "Consumers-as-Producers"?

Before concluding, let us examine a possible objection to the idea that "consumers as producers" is an important new feature created by modern computers and the Internet. The objection points out, correctly, that production from home is nothing new.[61] The term "economics" itself comes from the Greek word for household, with consumption and production thus together at the etymological root of the economics discipline. Pre-factory production, such as farming, weaving, and smithing, typically occurred at home. Retail establishments have historically often featured the shop on the first floor with the family living above. Many small businesses in the physical world today are based at home, including landscape services, solo plumbers, or accountants, and so on.

For consumer protection law, however, there are important distinctions between this history and today for reasons of scale, geographic scope, and the visibility of possible violations. On the issue of scale, the term "personal mainframe" is intended to convey what is different today. Individuals today own the computing power of a corporate mainframe from a decade ago. Individuals at home, even in their spare time, can thus produce a quantity and quality of information goods that match the historical profile of medium or large enterprises. Those enterprises are historically subject to enforcement under consumer

[59] For CAN-SPAM, the risk of harassing enforcement is currently low. The only private right of action is for Internet service providers, who have to date sued large spammers and not individuals who occasionally send an email that might be considered "commercial." 15 U.S.C. § 7706(g). If the law were amended in the future to allow a private right of action for any recipient and there were statutory minimum damages, then there would be the risk of bounty hunters who would sue consumers-as-producers who inadvertently cross the line into commercial email.

[60] Pierce (1998). See Garvin, supra note 2, at 297–298 (discussing literature about whether to have small business exceptions).

[61] Thanks to Professor Naomi Cahn for emphasizing this point.

protection laws, but in the Web 2.0 world, much of the "production" is done by individuals working at home in a setting not historically regulated in the same way. The small scale of the activity is therefore less likely to be a defense for products of the personal mainframe.

Conclusions

The geographic scope of home production is a function both of the personal mainframe and of the Internet. The typical home enterprise historically has served a local market, such as through personal services (such as a plumber), a retail store, or sales through local classified ads or flea markets. The personal mainframe means that an individual at home can produce at a scale that quite possibly outstrips local demand. Perhaps even more importantly, sales through the Internet mean that a seller from home, such as on eBay, reaches a global market. From the point of view of the producer, this global reach has enormous economic advantages because of the expanded pool of buyers. The global reach also has severe regulatory disadvantages, however. Now the producer has to consider whether enforcers in any relevant jurisdiction will seek to enforce consumer protection or other laws.

Consumers-as-producers confront the visibility of much online activity to go along with this multiplicity of possible enforcers. Home-based producers in the physical world often create only a meager evidentiary record about whether the seller broke the law. For instance, there may be no clear written contract about what a plumber promised to do and no clear evidence about whether the plumber's repairs were defective. By contrast, the consumer protection rules discussed in Part II all tend to produce clear evidence of violations by consumers-as-producers:

1. Lack of a privacy policy will be easy to detect on a web site.
2. Failure to comply with CAN-SPAM can be proven by anyone who saves the illegal commercial email.
3. A misleading advertisement on the web can be easily saved to a user's computer.
4. A political blog that fails to follow FEC rules will be subject both to easy detection (the required FEC filings will not be posted on the web) and incentives for complaints (partisans of the opposing party have reason to file a complaint).

There is thus considerably greater urgency to clarify consumer protection law for online consumers-as-producers than for traditional home producers who usually sell locally, on a small scale, and with less evidence of violations. Online consumers-as-producers are much more able to produce at a large scale, they have their activities visible in multiple jurisdictions, and they often produce clear evidence of violations as a by-product of online technology. It is thus true that consumers have also been producers since at least the time of the Greeks and the birth of "economics." But, the modern form of consumer-as-producers means that it is newly important to examine which laws historically designed to apply either to "consumers" or "producers" should apply to those who are both.

Acknowledgements For comments on earlier drafts, my thanks to participants at the Boalt Conference on DRM and Consumer Protection, the 2007 Freedom-to-Connect Conference, the Institute for Information Law Conference on the Place of the iConsumer in EU and US Law, and faculty workshops at the George Washington University Law School and the Moritz College of Law. My thanks for helpful discussions with Yochai Benkler, Ed Black, Julie Cohen, John Duffy, Natali Harberger, Robert Pitofsky, John Podesta, Pamela Samuelson, and Marc Spindelman, and for excellent research assistance by Ryan Coyer and especially Lauren Dubick, who played an unusually large role during the early phases of this project. My thanks as well to the Moritz College of Law and to the Center for American Progress for supporting the conference on "The Internet and the Future of Consumer Protection," from which the current paper emerged.

References

Broache, A. (2007). *Lobby Bill spares political bloggers*, CNET News, Jan. 19, 2007: http://news.com.com/Lobby+bill+spares+political+bloggers/2100-1028_3-6151519.html (discussing debate on Section 220 of S.1, a lobbying reform bill).

Carl, W. (2006). FTC response on word of mouth marketing regarding disclosure: http://wom-study.blogspot.com/2006/12/ftc-response-on-word-of-mouth.html (analyzing the Engle speech).

Center for Democracy & Technology and Institute, for Politics, Democracy & the Internet (2005). *Joint statement of "principles" relating to notice of proposed rulemaking 2005-10, the internet: definitions of "public communication" and "generic campaign activity' and disclaimers*, June 3, 2005: http://www.cdt.org/speech/political/20050603cdt-ipdi.pdf (collecting 1,115 signatures from advocacy groups, bloggers, and other individuals with diverse political viewpoints) [Hereinafter "Joint Statement of Principles"].

Engle, M. (2006). Word of mouth advertising and FTC advertising law. *Word of Mouth Marketing Association, Summit 2006*: http://www.womma.org/summit2/presentations/Engle.pdf.

Federal Trade Commission (2000a). *Advertising and marketing on the internet: rules of the road*, 2: http://www.ftc.gov/bcp/conline/pubs/buspubs/ruleroad.pdf. ("..claims must be substantiated, especially when they concern health, safety, or performance.").

Federal Trade Commission (May 2000b). *Dot Com disclosures*: www.ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.html.

Garvin, L. (2005). Small business and the false dichotomies of contract law. *Wake Forest Law Review*, *40*, 302–368.

Goldstein, A. (1999). *Long reach into patients' privacy; new uses of data illustrate potential benefits, hazards*. Washington Post, Aug. 23, 1999, at A1 (strict Maine medical privacy law repealed two weeks after taking effect).

Internet Communications (2006). *Federal Register*, *71*, 18,589–18,591 (Apr. 12).

Krebs, B. (2006). *In the fight against spam email, Goliath wins again*. Washington Post, May 17, 2006, at A1.

Lenhard, R., & Weintraub, E. (2006). *FEC internet rulemaking—background and FAQ*, Mar. 27, 2006: http://www.fec.gov/members/lenhard/speeches/statement20060327.pdf.

National Consumers League (2006). *A call for action: Report from the National Consumers League Anti-Phishing Retreat*, available at http://www.nclnet.org/news/2006/Final%20NCL%20Phishing%20Report.pdf.

Physorg.com. (2006). *For FTC, e-commerce means managing "mice"*, July 25, 2006: http://www.physorg.com/news73065889.html.

Pierce Jr., R. (1998). Small is not beautiful: The case against special regulatory treatment of small firms. *Administrative Law Review*, *50*, 537.

Singel, R. (2006). *Under attack, spam fighter folds*. Wired News, May 16, 2006: http://www.wired.com/news/technology/0,70913-0.html.

Swire, P. P. (1998). *Of elephants, mice, and privacy: International choice of law and the internet*. 32 The International Lawyer 991.

Swire, P. P. (2003). *Trustwrap: The importance of legal rules for e-commerce and internet privacy*. 54 Hastings L.J., 847.

Swire, P. P. (2005). *Elephants and mice revisited: Law and choice of law on the internet*. 153 U. Penn. L. Rev. 1975.

Swire, P. P. (2006). *The internet and the future of consumer protection*. Center for American Progress, July 24, *available at* http://www.americanprogress.org/issues/2006/07/internet.html.

Swire, P. P. (2008). *No cop on the beat: Underenforcement in e-commerce and cybercrime*. J. Telecomm. & High Technology L. (forthcoming), available at http://ssrn.com/abstract=1135704.

Swire, P. P., & Litan, R. E. (1998). None of your business: world data flows, e-commerce, and the European privacy directive. 45–49.