William & Mary Bill of Rights Journal

Volume 19 (2010-2011)
Issue 4

Article 7

May 2011

Campaign Disclosure, Privacy and Transparency

Deborah G. Johnson

Priscilla M. Regan

Kent Wayland

CAMPAIGN DISCLOSURE, PRIVACY AND TRANSPARENCY

Deborah G. Johnson, Priscilla M. Regan, and Kent Wayland*

INTRODUCTION

The United States has a long history of creating "public records" and viewing at least some of these as an essential part of government accountability.[1] Public records minimize opportunities for secrecy which might shield the actions of elected and appointed officials from public scrutiny. Historically, decisions to require public disclosure of information were made with particular limited purposes in mind: purposes associated with the public or democratic value of the disclosure.[2] Freedom of Information Act requirements, at both the federal and state levels, further opened access to government information and facilitated further disclosures of government information.[3] The Internet has exponentially escalated access to public records; information posted on the Internet is effectively broadcasted to anyone in the world who may be interested. The interested viewers may have benign, nefarious or legitimate reasons for being interested, and their interests may or may not be related to the original purpose for making the information public. Property tax records, professional licenses, parking tickets, sex offender databases, court records, and campaign disclosure are all good examples of such public records.[4]

As public records have been made available in computerized form and posted on the Internet, public concerns about protecting the privacy of personally identifiable information in these records have intensified. Before computers and information

---

* The authors are, respectively, Anne Shirley Carter Olsson Professor of Applied Ethics, School of Engineering and Applied Science, University of Virginia; Professor, Department of Public and International Affairs, George Mason University; Research Associate, School of Engineering and Applied Science, University of Virginia. William & Mary Bill of Rights Journal Symposium: Privacy, Democracy, and Elections, Williamsburg, Virginia, October 22, 2010. This material is based upon work supported by the National Science Foundation under Grant Number 0823363. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

[1] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON 127, 133 (2004).

[2] *See, e.g.* Michael Hoefges et al., *Privacy Rights Versus FOIA Disclosure Policy: The "Uses and Effects" Double Standard in Access to Personally-Identifiable Information in Government Records*, 12 WM. & MARY BILL RTS. J. 1, 2–3 (2003) ("Congress recognized the important need for citizens in a democracy to have access to government information in order to participate in self-rule.").

[3] *See id*. at 9.

[4] *See id. passim*.

technology, those who wished to see and copy information in public records had to traipse to a public building, request a record, wait for the staff to find it, carefully read through the record to find the item(s) of interest, and then copy the desired information manually.[5] The physical presence and labor involved resulted in "practical obscurity,"[6] that is, the work involved in obtaining access and duplicating information had the effect of protecting the privacy of the information. In the networked world, those built-in protections are removed and there is little or no obscurity. Records can be easily accessed, searched, analyzed, and reconstituted in new forms from nearly anywhere in the world. As early as 1989 in *Department of Justice v. Reporters Committee for Freedom of the Press*, the Supreme Court recognized that "there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[7] In that decision, the court held that rap sheets were not public information for the purposes of the Freedom of Information Act, recognizing "the privacy interest in keeping personal facts away from the public eye"[8] and "the privacy interest in maintaining . . . [its] 'practical obscurity.'"[9]

Public records or not, the ease of access to personal information made possible by information technology and the Internet has resulted in what Joel Reidenberg refers to as the "transparent citizen,"[10] what Dan Solove terms the "digital person,"[11] and what Jeffrey Rosen sees as the "unwanted gaze."[12] Personally identifiable information is somewhat up for grabs by those who have money, time, technological skills, and motive. Although the contours and implications of "information societies" have been and continue to be identified, analyzed, and critiqued, the radical shift in what it means for information to be in "public records" is often noted but less often analyzed.[13] An important implication of this shift is an intensification of the tension between privacy and transparency. As Joel Reidenberg points out, the "scope of transparency and the ease of re-purposing are a surprise to data subjects and the public at large."[14] A

---

[5] *See* SOLOVE, *supra* note 1, at 131 ("For a long time, public records have been accessible only in the various localities in which they were kept.").

[6] Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762 (1989) (internal quotations marks omitted).

[7] *Id.* at 764.

[8] *Id.* at 769.

[9] *Id.* at 762.

[10] Joel R. Reidenberg, The Transparent Citizen and the Rule of Law, Address Before the Berkman Ctr. for Internet & Soc'y (Feb. 11, 2010), http://cyber.law.harvard.edu/interactive/events/lawlab/2010/02/reidenberg.

[11] SOLOVE, *supra* note 1.

[12] JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2000).

[13] *See, e.g.*, SOLOVE, *supra* note 1, at 131–32 (observing that the "reality is rapidly changing").

[14] Reidenberg, *supra* note 10, at 8.

powerful example of this is the release of publicly available information about Justice Scalia by Fordham law students.[15] The new landscape of information accessibility and flow calls into question whether the common good requires new principles, controls, and regulation.[16]

Most of the debate and writing that addresses the conflict between privacy and public records has centered on the issue of court records[17] and the issue of community notification laws for sex offenders, also called Megan's Laws.[18] Dan Solove notes that courts can seal court records if the importance of confidentiality in a particular context outweighs the need for public access;[19] a trial court can permit a plaintiff to proceed with the use of a pseudonym;[20] and courts can permit anonymous juries.[21] However, most of these decisions about the privacy accorded in trials are at the judge's discretion.[22] In 2002, the National Center for State Courts and the Justice Management Institute prepared draft guidelines for public access to court records, particularly in light of technological innovations.[23] They based their recommendations on the principle that although a "general rule" for access should be the same "whether the Court record is in paper or electronic form," the nature of some information in court records may mean that "remote public access to the information in electronic form may be inappropriate."[24] This was then followed by publication of final guidelines, with particular attention to family court records, in 2005.[25] State Megan's Laws, which require public disclosure of information about the location of convicted sex offenders after

---

[15] *E.g.*, Noam Cohen, *Law Students Teach Scalia About Privacy and the Web*, N.Y. TIMES, May 18, 2009, at B3 (explaining how Fordham law students were able to create a dossier about Justice Scalia that included his home address and phone number, his wife's personal e-mail address, and his favorite TV shows and food from sources on the Internet).

[16] *See, e.g.*, Julie E. Cohen, *Privacy, Ideology, and Technology: A Response to Jeffrey Rosen*, 89 GEO. L. J. 2029, 2035 (2001) (observing the existence of "strong arguments against placing limits on the collection and use of information" (emphasis omitted)).

[17] *See, e.g.*, Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1157–60 (2002) (describing jurisprudence on access to court records).

[18] *See, e.g.*, *id.* at 1148–49 (describing the reach of federal and state community notification laws).

[19] *Id.* at 1159.

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] NAT'L CTR. FOR STATE COURTS & JUSTICE MGMT. INST., PUBLIC ACCESS TO COURT RECORDS: GUIDELINES FOR POLICY DEVELOPMENT BY STATE COURTS (2002), *available at* http://www.aija.org.au/tech3/program/presentations/slater/sjiGuide.pdf.

[24] *Id.* at 1.

[25] ALAN CARLSON & MARTHA WADE STEKETEE, PUBLIC ACCESS TO COURT RECORDS: IMPLEMENTING THE CCJ/COSCA GUIDELINES, at vii, 29–30 (2005), *available at* http://www.jmijustice.org/publications/implementing-the-ccj-cosca-guidelines-on-public-access-to-court-records/view.

they have served their sentence, also raise questions about online access. Some courts allow wide public access, while others are more cautious.[26]

In general, as Hoefges points out, the policy discussions about balancing or reconciling the importance of public disclosure with the protection of individual privacy focus in large part on the purposes for which the information is likely to be used and the consequences of such uses for the individuals named in the record.[27] Indeed, the question of subsequent uses of the personal information and the consequences for the individuals involved are quite pertinent in all debates about public records.[28] For example, in a 1994 case the Supreme Court ruled that there was not a FOIA-related public interest in disclosing federal employees' home addresses to labor unions because such disclosure did not reveal anything substantively related to official agency actions.[29] Critics have argued that the court's approach has "allowed minimal privacy invasions to tip the scales in favor of nondisclosure."[30] Nevertheless, this continues to be negotiated depending on the context. Drawing the line between the public interest in disclosure and the interest in privacy has proved to be a challenge.

Campaign finance disclosure (CFD) is an important domain in which electronic reporting has aggravated the tension between privacy and transparency. As a mechanism of accountability, CFD comes directly into conflict with privacy. On the one hand, because the secret ballot and associational privacy are at stake,[31] there is a strong case to be made for privacy. On the other hand, the privacy interest is often not supported by constitutional or statutory law,[32] and earlier Supreme Court rulings clearly supported the principle that "individual privacy interests can be outweighed by public interests that are served by government collection and use of personally-identifiable data."[33] CFD is especially important here because the secret ballot and associational privacy are not just individual privacy interests but are public goods essential to democratic governance.[34] In other words, CFD may constitute one of the strongest cases for privacy protection to trump disclosure.

---

[26] *See* Solove, *supra* note 17, at 1183–84 (noting "courts are deeply divided about whether to adhere to the secrecy paradigm").

[27] Hoefges et al., *supra* note 2, at 5.

[28] *See id.* at 6–7 (describing Supreme Court jurisprudence regarding subsequent uses and consequences).

[29] Dep't of Def. v. Fed. Labor Relations Auth., 510 U.S. 487, 502 (1994).

[30] Hoefges et al., *supra* note 2, at 39.

[31] *See* William McGeveran, *Mrs. McIntyre's Checkbook: Privacy Costs of Political Contribution Disclosure*, 6 U. PA. J. CONST. L. 1, 20–21 (2003) (arguing that such disclosure "may cause concrete harms when others learn about an individual's political convictions").

[32] *See id.* at 20–22 ("The Supreme Court has never clearly articulated an independent constitutional right to information privacy.").

[33] Hoefges et al., *supra* note 2, at 53.

[34] *See* Universal Declaration of Human Rights, G.A. Res. 217 (III) A, art. 21(3), U.N. Doc. A/RES/217(III) (Dec. 10, 1948) ("The will of the people shall be the basis of the authority of government . . . and shall be held by secret vote . . . .").

I. RATIONALE FOR PRIVACY IN VOTING

Privacy is an important but elusive concept that is arguably important in democratic government. Julie Cohen, for example, sees a strong connection between information privacy, which promotes individual autonomy and self-development, and vigorous public debate.[35] Paul Schwartz also views information privacy as a conditional requirement for deliberative democracy.[36] Priscilla Regan argues that privacy is not just an individual value but also a public value; it is important for democratic political systems in being essential for the exercise of a number of First Amendment rights, in establishing boundaries on the exercise of governmental power, and also in enabling the development of some commonality among individuals, which is necessary to unite a political community.[37]

However, in focusing here on CFD, the importance of privacy to democracy is found in its connection to the right to vote. The importance of privacy in the domain of voting has been affirmed in a diverse set of court decisions that protect associational privacy and diminish the amount of information voters must reveal in order to exercise their right to vote. Associational privacy is seen as essential for citizens to form their opinions in an exploratory, unencumbered, tentative, non-punitive manner.[38] In *NAACP v. Alabama*, the Supreme Court struck down a state statute which required the NAACP to disclose the names and addresses of its members, ruling that there is a "vital relationship between freedom to associate and privacy in one's associations."[39] In 1993, the Fourth Circuit Court of Appeals applied somewhat similar logic in ruling that the Virginia requirement that voters provide their Social Security number (SSN) was unconstitutional because it forced people to risk public disclosure of the SSN in order to vote.[40] Virginia voter registration lists were required to be open to "public inspection"[41] which the plaintiff argued was an unconstitutional burden on his right to vote.[42] The court noted that the harm to an individual from the disclosure of a SSN

---

[35] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423–27 (2000).

[36] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1651 (1999) (arguing that "absent strong rules for information privacy, Americans will hesitate to engage in . . . activity likely to promote democratic self-rule").

[37] PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 225–27 (1995) ("Privacy has value not just to individuals as individuals or to all individuals in common but also to the democratic political system.").

[38] *See* NAACP v. Alabama, 357 U.S. 449, 462 (1958) ("It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute a restraint a freedom of association.").

[39] *Id.* at 462.

[40] Greidinger v. Davis, 988 F.2d 1344, 1355 (4th Cir. 1993).

[41] There were restrictions on who could obtain copies of the lists and the purposes were limited to those that were deemed election-related. *See* VA. CODE ANN. § 24.2-406 (1950).

[42] *Greidinger*, 988 F.2d at 1348.

was "alarming and potentially financially ruinous."[43] The court ruled "that the fundamental right to vote was substantially burdened by the provision requiring public disclosure of the [SSN]" and that "there was no compelling state interest in [its] public disclosure."[44] Virginia then passed a law preventing public inspection of SSN although it was still collected by the state for voter registration purposes.[45]

Courts have recognized that the marketplace of ideas in which individuals form their opinions, including those about political candidates, includes the right of speakers to remain anonymous. For example, in *McIntyre v. Ohio Elections Commission*,[46] the Court ruled that "[u]nder our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority."[47] If speakers are entitled to be anonymous in political expression, then one could argue by extension that voting is a form of public expression as well, and should, therefore, be anonymous. Indeed voting has been protected by practice since the Australian ballot, which has been used in the United States since the late nineteenth century.[48] The rationale behind the secret ballot is that one should not be open to retaliation or need to explain one's vote; one's vote should be confidential, known in effect only to oneself.[49] When women gained the vote, it was noted that the secrecy of the ballot ensured that women would be voting for themselves, not for their husbands.[50]

This is not to say that the courts or governments have not compromised in protecting the confidentiality of voting choice on the ballot. States require individuals to register to vote, and have made the registry a public record, as mentioned before in the case involving disclosure of SSNs included in Virginia's voter registry.[51] Although this may appear to be inconsistent with the secret ballot, voter registration signifies the fact that one votes as a citizen, a public person if you will.

Voters do, then, have to reveal personal information in order to vote, but just what information they have to reveal and how it is treated is a complicated matter. Depending upon the state, the voter registry may reveal "one's political party affiliation, date of birth, place of birth, e-mail address, home address, telephone number, and sometimes one's Social Security number."[52]

---

[43] *Id.* at 1354.

[44] Robert Gellman, *Public Records—Access, Privacy, and Public Policy: A Discussion Paper*, 12 GOV'T INFO. Q. 391, 404 (1995) (describing the holding from *Greidinger*).

[45] *Id.*

[46] 514 U.S. 334 (1995).

[47] *Id.* at 357.

[48] ELDON COBB EVANS, A HISTORY OF THE AUSTRALIAN BALLOT SYSTEM IN THE UNITED STATES, 27–28 (1917).

[49] *See id.* at 21–24.

[50] *See generally* THE ENCYCLOPEDIA OF SOCIAL REFORM 1405 (William D. P. Bliss eds., London, Funk & Wagnalls Co. 1897).

[51] Greidinger v. Davis, 988 F.2d 1344, 1354 (1993).

[52] Solove, *supra* note 17, at 1144 (internal citations omitted).

Some states have restricted access to public record information, generally to exclude access for the commercial uses of soliciting business or marketing services to the public. More than half of the states prohibit the commercial use of voter registration records.[53] For example, "California [allows] voter registration lists [to] be released to candidates, political committees, or for 'election, scholarly, journalistic, political, or governmental purposes.'"[54] Florida allows or permits use of lists of registered voters for purposes "related to elections, political or governmental activities, voter registration, or law enforcement."[55] Similar restrictions apply to information about federal campaign contributions. The Federal Election Campaign Act states that reports of contributors to political committees are "available for public inspection . . . except that any information copied from such reports . . . may not be sold or used by any person for the purpose of soliciting contributions or for commercial purposes . . . ."[56]

The landscape of court decisions is complicated, though it indicates that the importance of privacy in voting is well recognized in the law. However, privacy protection is not ironclad. There are many opportunities for privacy erosion, especially at the state level.

II. RATIONALE FOR TRANSPARENCY IN CAMPAIGN FINANCING

The idea of transparency in campaign financing is quite consistent with the famous quote from James Madison's letter to W.T. Barry:

> A popular Government, without popular information, or the means of acquiring it, is but a prologue to a Farce or a Tragedy; or perhaps, both. Knowledge will forever govern ignorance: and a people who means to be their own Governors, must arm themselves with the power which knowledge gives.[57]

No other context is as important to democracy than elections to public office. If knowledge is to prevail over ignorance, then citizens must be informed about candidates and campaigns. From the early twentieth century, knowledge about who was contributing to electoral campaigns has been framed as a way of ensuring fair and open elections, addressing concerns about undue influence by the more economically

---

[53] Philip N. Howard, *Deep Democracy, Thin Citizenship: The Impact of Digital Media in Political Campaign Strategy*, 597 ANNALS AM. ACAD. POL. & SOC. SCI. 153, 166 (2005).

[54] Solove, *supra* note 17, at 1170 n.216 (quoting CAL. ELEC. CODE § 2194(a)(2) (West 2002)).

[55] *Id.* (quoting FLA. STAT. ANN. § 98.095(2) (West 2002)).

[56] Federal Election Campaign Act of 1971, Pub. L. No. 92-225, § 308(a)(4), 86 Stat. 3, 17 (1972) (codified as amended in 2 U.S.C. § 438(a)(4) (2006)).

[57] Letter from James Madison to W.T. Barry (Aug. 4, 1822), *in* 9 WRITINGS OF JAMES MADISON 103 (Gaillard Hunt ed., 1910).

advantaged and privileged individuals, and preventing corruption of the electoral process.[58] The 1910 Publicity Act required House campaign committees to disclose contributors in excess of $100 within thirty days of an election;[59] in 1911 this was extended to Senate candidates.[60] The 1925 Federal Corrupt Practices Act required disclosure in non-election years as well.[61] The 1971 Federal Election Campaign Act (FECA) tightened requirements for campaign finance reporting and disclosure and also made them applicable to primary elections.[62] In 1974 FECA was amended to require "candidates to file quarterly reports on their contributions and expenditures with the [Federal Elections Commission (FEC)],"[63] and made these records available to the public.[64]

The FEC is required to make these reports available to the public within forty-eight hours of receipt.[65] But, the law prohibits the sale or use of information from these records for purposes of soliciting contributions, including political or charitable contributions, and for any commercial purposes.[66] The FEC regulations state that use of FEC information in "newspapers, magazines, books, or similar communications is permissible as long as the principal purpose . . . is not to communicate any contributor information . . . [to] solicit[ ] contributions or for other commercial purposes."[67] In a 1992 case, the D.C. Circuit Court ruled that these restrictions served "an important governmental interest[ ] in reserving the value of the contributor list to the political committee that creates it."[68] It is worth noting that the proprietary interest of the campaign organizations provided the motivation for the protection, not the privacy interests of the contributors.[69]

In most of these laws, disclosure requirements were part of a larger package of controls over campaign financing that also included some restrictions on both contributions and expenditures.[70] However, a landmark Supreme Court case in 1976 challenged the constitutional viability of this three-pronged approach of contribution limitations, expenditure restrictions and disclosure requirements by permitting limits on campaign contributions as a way to reduce the reality or appearance of corruption in the political

---

[58] For a short history of the campaign finance laws, see VICTORIA A. FARRAR-MYERS & DIANA DWYRE, LIMITS AND LOOPHOLES: THE QUEST FOR MONEY, FREE SPEECH, AND FAIR ELECTIONS 8–19 (2008).

[59] Act of Jun. 25, 1910, ch. 392, § 6, 36 Stat. 822, 823.

[60] Act of Aug. 19, 1911, ch. 33, § 5, 37 Stat. 25, 25–27.

[61] Federal Corrupt Practices Act of 1925, ch. 368, tit. III, § 305(a), 43 Stat. 1053, 1070.

[62] *Id.* at 11.

[63] *Id.* at 11–12.

[64] FARRAR-MYERS & DWYRE, *supra* note 58, at 12.

[65] 2 U.S.C. § 438(a)(4) (2006).

[66] *Id.*

[67] 11 C.F.R. § 104.15(c) (2011).

[68] FEC v. Int'l Funding Inst., 969 F.2d 1110, 1118 (D.C. Cir.), *cert. denied*, 506 U.S. 1001 (1992).

[69] Gellman, *supra* note 44, 414.

[70] *See, e.g.*, *Int'l Funding Inst.*, 969 F.2d at 1117.

system and validating disclosure requirements,[71] but invalidated limits on campaign expenditures as an unconstitutional infringement of the candidate's free speech.[72] One thrust of this ruling has been the creation of ways around the contributions restrictions, often by finding loopholes that allow money to be funneled through different organizations.[73] Another thrust has been to elevate the importance of the disclosure requirements, which are clearly viewed as constitutional, as a means of tracking the myriad routes that contributions can take.[74]

The most recent Supreme Court decision regarding the constitutionality of campaign finance requirements and addressing the question of disclosure requirements is *Citizens United v. Federal Election Commission*.[75] With respect to disclosure, the Court specifically noted:

> With the advent of the Internet, prompt disclosure of expenditures can provide shareholders and citizens with the information needed to hold corporations and elected officials accountable for their positions and supporters. Shareholders can determine whether their corporation's political speech advances the corporation's interest in making profits, and citizens can see whether elected officials are "'in the pocket' of so-called moneyed interests."[76]

The Court noted that the *McConnell* decision recognized that disclosure requirements "would be unconstitutional as applied to an organization if there were a reasonable probability that the group's members would face threats, harassment, or reprisals if their names were disclosed,"[77] and that "the examples cited by *amici* [were] cause for concern."[78] However, the Court concluded that Citizens United did not offer "evidence that its members . . . face[d] similar threats or reprisals."[79]

---

[71] Buckley v. Valeo, 424 U.S. 1, 55 (1976) (per curiam) ("The interest in alleviating the corrupting influence of large contributions is served by . . . contribution limitations and disclosure provisions . . . .").

[72] *Id.* at 58–59.

[73] *Id.* at 252–53 (Burger, C.J., dissenting) (predicting "that the Court's holding will invite avoidance").

[74] *Id.* at 76.

[75] 130 S. Ct. 876 (2010). The Court, in an 8-1 ruling, held valid a statute requiring any person that spends more than $10,000 in a year to produce or air an election ad covered by federal restrictions must file a report with the Federal Election Commission disclosing the names and addresses of anyone who contributed $10,000 or more to the ad's preparation or distribution. *See id.* at 914.

[76] *Id.* at 905–06 (quoting McConnell v. FEC, 540 U.S. 93, 259 (2003) (Scalia, J., concurring in part and dissenting in part)).

[77] *Id.* at 916.

[78] *Id.* ("Some *amici* point to recent events in which donors to certain causes were blacklisted, threatened, or otherwise targeted for retaliation.").

[79] *Id.*

Following the Court's ruling, bills were introduced to expand and clarify disclosure requirements, including the "Democracy is Strengthened by Casting Light on Spending in Elections (DISCLOSE) Act."[80] This Act includes a provision obligating many advocacy organizations to release the identities of many of their donors, while exempting organizations that have over 500,000 members, have received section 501(c) of the Internal Revenue Code tax exemptions for the previous ten years, have a presence in all fifty states, and whose funding from corporations and unions is less than fifteen percent.[81] The ACLU and other opponents of this Act argue that the bill inequitably suppresses only the speech of smaller organizations that might be more controversial and compromises the anonymity of small donors.[82] In a letter to the Senate, the ACLU stated,"The DISCLOSE Act blurs the line between issue and campaign advocacy and puts at risk of exposure the heretofore confidential donor records of millions of Americans and thousands of legitimate non-profit advocacy organizations."[83] The letter also states that "disclosure requirements should not have a chilling effect on the exercise of rights of expression and association, especially in the case of controversial political groups."[84]

The debate over the DISCLOSE Act is illustrative of a broader concern that the availability of public records online will lead to the transformation of activities designed for one purpose into new forms of surveillance. In the case of campaign finance, what originated as a system of accountability based on the idea that transparency would help to control inappropriate influence on political candidates, has turned into a system of monitoring and targeting (i.e. surveillance) of campaign contributors. In effect, the lens of CFD has turned from campaigns and candidates to (include) donors.

III. TRANSPARENCY AS A HOUSE OF MIRRORS

The transformation that has occurred in CFD is in large part the result of moving public records into an electronic medium. When "public records" are constituted in this medium, they can be used in ways that were practically impossible before. Since transparency involves, by definition, the revelation of information, the tension between transparency and privacy arises regardless of medium. However, this tension is exacerbated and reconfigured in an electronic medium. The reconfiguration means that in order to address the issues that arise and achieve an appropriate balance, an understanding of the nature of the electronic medium is essential.

---

[80] Democracy is Strengthened by Casting Light on Spending in Elections (DISCLOSE) Act, H.R. 5175, 111th Cong. (2010).

[81] *Id.* § 211(c)(27).

[82] *See, e.g.*, Letter from Laura W. Murphy, Director of the ACLU, to the United States Senate (July 23, 2010), *available at* http://www.aclu.org/files/assets/Ltr_to_Senate_re_ACLU_opposes_DISCLOSE_Act.pdf.

[83] *Id.*

[84] *Id.* at 1.

In what follows, we make use of a metaphor to conceptualize what happens when public records are constituted in an electronic medium. Again we focus on CFD as a case illustrating how the tension between transparency and privacy is configured. *The metaphor involves viewing the processes of developing accounts of campaigns, candidates, and donors as analogous to the activities that occur in a house of mirrors.* The metaphor is a heuristic device used here to tease out (reveal) the myriad ways that information is transformed and repurposed in the electronic medium. Use of the metaphor suggests that we ought to be cautious in presuming that transparency is transparent or in claiming that transparency in itself is a viable form of accountability for democratic institutions.

What does it mean to say that the production of CFD accounts is analogous to what goes on in a house of mirrors? A house of mirrors is full of reflection, refraction, multiplication of images, and unpredictable perspectives; a person standing in a house of mirrors sees aspects of their body seemingly distorted, that is, elongated, shortened, exaggerated, and fragmented. A house of mirrors is a complex of imagery, with bouncing, highlighting, and shading of images that produce a surprising experience. An individual sees an image of him or herself out of whack with their ordinary sense of self. Of course, the seeming distortion is far from random; it is the result of the way the mirrors have been made, the placement of the mirrors in the architecture of a building, the lighting, the way the house has "billed" (advertized) to the public, and so on. Houses of mirrors are created explicitly for fun—they are often referred to as "fun houses."

The design and architecture of a house of mirrors parallels the structures and affordances of information technology and the Internet. Paper and ink data have very different properties from electronic data posted on the Internet. Playing out the metaphor of a house of mirrors, at least four processes can be identified in the production of Internet instrumented information systems: entry, bouncing, highlighting and shading, and rendering. The outcome of these processes—the rendering—is an account (or accounts) delivered in the name of transparency, though highly processed and infused with normative assumptions and values.

A. Entry

When a person enters a house of mirrors, a reflection of the person is constituted in a mirror (or mirrors). Similarly, when someone donates to a campaign (in effect entering the CFD system), the campaign creates a record.[85] This initial record-creation is done in response to, and in accordance with, legal requirements. The legal requirements specify what personal information donors must supply[86] and the system is set up so that one cannot donate unless one provides this information.[87] Campaigns are

---

[85] *See* 2 U.S.C. § 434(a) (2006) (setting forth the FEC's reporting requirements).

[86] *Id.* § 434(b) (setting forth the content required to be disclosed in FEC reports).

[87] *Id.*

required to gather, record, and submit this information to the FEC.[88] Unlike a house of mirrors in which entry is typically accompanied by a reflection seen by the entrant, donors do not immediately "see" the record created in the campaign data base. Nevertheless, one has been created and will, in a short period of time, be posted on the Internet.[89] Interestingly, the image created in CFD is instantaneously multiplied in the sense that the donation is seen as a reflection both of the campaign and the donor.

Donors are required to supply their name, employer, occupation, home address, and the amount donated.[90] In this respect, the reflection of the donor and campaign is selective and limited. It is a reduction of the person. In requiring certain information and not other information, CFD law singles out certain aspects of donors that are deemed relevant. The information provided doesn't reveal a donor's motivation in contributing to the campaign; it doesn't tell the percentage of the person's total wealth that is donated; it doesn't disclose the person's age, gender, or party affiliation. The required items might be thought of as establishing a donor's identity vis-a-vis CFD. Importantly, the required items have not been arbitrarily selected.

Particular information is required because of a set of assumptions that are made in CFD law about human nature, interests, and corruption. For example, the assumption seems to be that individuals with particular occupations have interests and might use money to try to influence campaigns to serve their interests.[91] Similarly, the requirement that one supply one's name and address seems to assume that individuals may want to hide their identity; hence their identity must be established.[92] In American democracy, some forms of influence are legitimate and others not. Embedded in these required elements are norms about "what matters" in political campaigns and what constitutes political corruption. Contributions from members of certain occupations and contributions of a certain size are somehow linked to inappropriate influence or influence that is relevant to the public (voters). This potentially inappropriate influence will, presumably, be counterbalanced if voters are able to see what the influences might be.

So, while the record created upon entering the CFD system is a reduction, it is a selective reduction based on assumptions about what is relevant and what is not for the purposes of accountability and fair elections. The parallel to a house of mirrors is with the architecture of the house which has been set up to produce oddly configured and fanciful reflections. Indeed, the parallel between the multiple, rearranged reflections produced in the house of mirrors and the selected and ordered display of information about donors in the CFD system captures some of the uncontrollability of information posted on the Internet. The campaign gathers data about its donors so as to produce an

---

[88] *Id.* § 434(a).

[89] *Id.* § 434(d)(2) (requiring documents to be made "accessible to be the public on the internet not later than 24 hours after the document is received by the Commission").

[90] *See id.* §§ 431(13), 432(c).

[91] *See, e.g.*, Ian Ayres, *Should Campaign Donors Be Identified?*, REGULATION, Summer 2001, at 12–14, *available at* http://www.cato.org/pubs/regulation/regv24n2/ayres.pdf.

[92] *Id.*

account of the campaign but the account reflects the donors.[93] In effect, the reflection is doubled.

B. Bouncing

In a house of mirrors, a person's (mirror-constituted) reflection moves from surface to surface, perhaps down hallways, into unseen corners and even into different, unrelated portions of the house. The reflection multiplies and each replication is an opportunity for additional contortion of the reflection; each replication is an opportunity for surprise. Once a record of a donation has been created by a campaign, merged with other information, and posted on the Web by the FEC, it can be, and often is, bounced from one location to another where it may reveal new aspects.[94] Donor/ campaign data can be copied, mined, and reposted endlessly.[95] It can move to unexpected places, with unpredicted results. The global scope of potential bouncing parallels the infinite regress of mirrors reflecting other mirrors.

In CFD, since the information is posted on public web sites,[96] data on individual donations bounce from the databases of the campaign to those of regulators to those of watchdog groups, journalists, law enforcement, neighbors, family and friends.[97] In this we see some of the primary affordances of information technology and the Internet.[98] At each of these places, the data can be easily and almost perfectly replicated and transmitted. Journalists, watchdog groups, other data repositories and even citizens can download subsets of the data or the entirety.[99] The data can be searched

---

[93] For example, Internet access to campaign donors is readily available on the FEC's website, searchable by contributor's name, city, state, zip code, business, date, and amount. *See Disclosure Data Search*, FED. ELECTIONS COMM'N, http://www.fec.gov/finance/disclosure/disclosure_data_search.shtml (last visited Apr. 10, 2011).

[94] *See* 2 U.S.C. § 434(a)(12) (2006) (allowing the FEC "to post . . . information on the Internet immediately upon receipt"); *see also* McGeveran, *supra* note 31, at 12 ("After the government makes this [political contribution] information conveniently available, private entities and the news media disseminate it further. Various independent advocacy groups use disclosure data to create sophisticated online databases of individual contributors.").

[95] McGeveran, *supra* note 31, at 13 ("Th[e] combination of campaign finance disclosure law, government administrative practices, and new technology makes information about individual political contributions much more widely and easily available . . . .").

[96] *See* 2 U.S.C. § 434(a)(11)(b) (establishing standards to mandate disclosure of contributions on the internet to be made publicly accessible within forty-eight hours).

[97] *See supra* note 93 and accompanying text.

[98] For a discussion of how information technology over the Internet provides wide publicity, see Danah Boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life*, *in* YOUTH, IDENTITY, AND DIGITAL MEDIA 124–26, 137–38 (David Buckingham ed., 2008) (arguing that the rise of the Internet and social network sites are "networked publics" that support sociability and "searchability").

[99] *See* McGeveran, *supra* note 31, at 11 ("Dramatically increased computerization has created digitized archives of personal data that are larger, more publicly accessible, and more

quickly,[100] and it can also be mined for relationships that might not be immediately apparent.[101] People can search within their neighborhood to find what their neighbors are doing.[102] Campaigns and political consultants can link the donation databases to other databases to better target fund-raising and advertising.[103] The dynamic and networked nature of the Internet means that the data can quickly be exposed to large audiences. And, the data persist in Web-linked databases, ever ready to be recalled when a person searches for them, ever ready to be mined or manipulated in new ways.

This movement from place to place (bouncing) is beyond the control of the person the data are about. Although not intended in the legislation creating CFD, the donor's loss of control of personal data is now "the price one pays" for making a donation. The price can be very high. Consider the 2008 California ballot initiative known as Proposition 8. It sought to ban gay marriage, and many groups poured resources into advertising for or against this controversial measure. Soon after it was passed, opponents of the ban, outraged with the result, sought to find out how campaign for the ban had succeeded. Thanks to state campaign finance laws, they were able to develop a robust database of people who funded the initiative's passage.[104] An enterprising and anonymous programmer mashed up the names and geographic locations of the donors with Google maps, producing www.eightmaps.com, a site where any visitor could see who in what neighborhoods contributed to the campaign.[105] As a result many individual supporters were targeted with insults, threats and boycotts.[106] Certainly those individuals never imagined that the result of their donation would be personal harassment on the apparent assumption that they were anti-gay zealots. This is one of the most salient illustrations of how a transparency system can turn into a surveillance system.

---

easily searched and analyzed than ever before. In the last five years, campaign contribution disclosure suddenly joined the trend of online compilation and availability." (internal footnotes omitted)).

[100] *See supra* note 93 and accompanying text.

[101] *See supra* note 99 and accompanying text.

[102] *See supra* notes 93, 99 and accompanying text.

[103] *See, e.g.*, Leslie Wayne, *Voter Profiles Selling Briskly as Privacy Issues are Raised*, N.Y. TIMES, Sept. 9, 2000, at A1 (reporting on Aristotle International, a company with the nation's largest voter data bank that provides detailed profiles of voters and sells them to politicians, as "one of the first companies to fully exploit the use of technology in the political system" (internal quotation marks omitted)). *But see* 2 U.S.C. § 438(a)(4) (2006) (prohibiting the sale or use of any information reported to the FEC for the purpose of "soliciting contributions or for commercial purposes").

[104] *See* Brad Stone, *Prop 8 Donor Web Site Shows Disclosure Law is 2-Edged Sword*, N.Y. TIMES, Feb. 8, 2009, at B3 (arguing that Eightmaps.com, a website that overlays personal data of Proposition 8 donors on a Google map, "is the latest, most striking example of how information collected through disclosure laws . . . may be undermining the democratic values that the regulations were to promote").

[105] *Id.*; *see also* PROP 8 MAPS, http://www.eightmaps.com (last visited Apr. 10, 2011) (with text accompanying map: "Proposition 8 changed the California state constitution to prohibit same-sex marriage. These are the people who donated in order to pass it.").

[106] *Id.*

In a house of mirrors the bouncing of images is intentionally designed to create fun. Explaining why donor data move so freely on the Internet is more complicated. The CFD system was created to make campaigns accountable and not intended to create public surveillance of donors.[107] Why, then, has this happened? Part of the story must be simply the affordances of the Internet, but why hasn't this affordance been constrained? Why, that is, has the situation been tolerated? Here we speculate that the free movement of donor data aligns with normative assumptions about the value and importance of transparency. In other words, on the face of it, transparency of donors may be seen as a good thing. It may also have been seen, as suggested earlier, as the price one has to pay for transparency of campaigns. In any case, to move now in the direction of hiding donor data involves stepping over a hurdle that was not exactly or intentionally placed. The hurdle to hiding donor data seems to have been an unintended consequence of the switch to an electronic medium.

C. Highlighting and Shading

The reflection that one sees in a house of mirrors highlights and shades various aspects of a person's body. As can be seen in the case of the California ballot initiative, as reflections of persons are bounced from place to place and re-contextualized and repurposed, various aspects of a person are highlighted and shaded. The highlighting and shading results from the nature of the electronic environment as well as from the contexts and purposes in which the data are used. As such, the highlighting and shading are unpredictable. Not only is an individual not in control of how their data are used, it is not possible to predict how, in fact, the data will be used.

The highlighting and shading can be illustrated with a simple example. If one searches on Google for "Kent Wayland" (one of the authors of this paper), one of the top results links to a database available at the *Huffington Post*, an online newspaper, where users may browse campaign donations with specially designed Web tools, by name, zip code, date of donation, campaign season, etc.[108] The database further displays recent political donations, downloaded from the FEC, repackaged and subject to indexing by Google's Web crawler.[109] Although Wayland's political activity and campaign donations are relatively minor, they make up a significant component of his online identity due to the high ranking Google gives these search results. Information on Wayland's contributions is not just bounced from site to site; his contributions become a highlighted aspect of his Web presence because of the combination of the way Google works, the *Huffington Post*'s popularity, and Wayland's other (in)activity: Wayland's name is not especially common, his Web presence is not

---

[107] *See* Richard Briffault, *Campaign Finance Disclosure 2.0*, 9 ELECTION L.J. 273, 286 (2010).

[108] *Huffpost Fundrace Results*, HUFFINGTON POST, http://fundrace.huffingtonpost.com/neighbors.php?type=name&lname=wayland&fname=kent (last visited Apr. 10, 2011).

[109] *Id.*

especially extensive, and the *Huffington Post* is recognized by Google's search engine as an especially popular site. This illustrates how the architecture of the Internet may shape a person's identity in a unpredictable way.

The press and reporters routinely scour disclosures for lines of influence and suggestions of a candidate's political leanings. Watchdog groups, too, pore over CFD information for threats to the public interest, or whatever other interest they are protecting.[110] Opposing candidates and opposition researchers scrutinize donor lists for any hint of scandal tied to individual donors—corrupt businessmen, perhaps, or ineligible donors.[111] Opponents may look for classes of donors, such as trial lawyers, health care organizations, or oil companies, who could shape or fit into a critical narrative about the candidate. In some cases, especially in major national races, a candidate may be forced to publicly denounce ill-fated acquaintances formed largely for financial expedience. Such was the case in the 2007 U.S. presidential primaries, when then-candidate Hillary Rodham Clinton decided to return $850,000 in funds raised for her campaign by the Democratic operative Norman Hsu, a con man charged and later convicted in a pyramid scheme that bilked investors out of $20 million.[112] Senator Clinton claimed she wasn't aware of Hsu's crimes but continues to face scrutiny regarding her relationship to him.[113]

In a house of mirrors, the mirrors may have been designed and positioned to elongate your legs reconfiguring them out of proportion or to change the shape of your head so that you are all eyes. Something parallel happens in CFD. Initially in CFD systems attention is drawn to the five required elements of one's identity, and when these items are posted on the Internet, they are combined and processed with other data, and put in contexts that highlight and shade aspects of a person of which that even the person may be unaware.

D. Rendering of Accounts

When a person exits a house of mirrors, the reflections, bouncing, highlighting and shading stops, though the person may well be left with a new perspective on himself or herself. The individual may remember a series of these images or a concatenation of images that make her see herself differently.

---

[110] *E.g.*, McGeveran, *supra* note 31, at 12–13.

[111] *E.g.*, *id.* at 12–13, 29; *see* Buckley v. Valeo, 424 U.S. 1, 67 (1975) (per curiam) ("[D]isclosure requirements deter actual corruption and avoid the appearance of corruption by exposing large contributions and expenditures to the light of publicity.").

[112] Benjamin Weiser, *Democratic Fund-Raiser Gets 24-Year Term for Fraud*, N.Y. TIMES, Sept. 29, 2009, at A28.

[113] John Solomon et al., *Clinton Campaign Cites Flawed Background Check: No Evidence of Fundraiser's Lawsuit or Bankruptcy Turned Up in Records Search, Spokesman Says*, WASH. POST, Sept. 12, 2007, at A3; Peter Flaherty, *Hsu Convicted But No Reckoning for Hillary*, NAT'L LEGAL & POL'Y CTR. (May 20, 2009, 3:00 PM), http://nlpc.org/stories/2009/05/20/hsu-convicted-no-reckoning-hillary.

In the CFD what results is not a memory of one's distorted body, but an account—usually many accounts—that has been rendered from the initial reflection (information gathered) being bounced, combined with other data, and highlighted and shaded. "Render" here carries the connotation of something (someone) being taken apart and then transformed into something different. The rendering(s) might be likened to a cubist or surrealist portrait of a person. Features are selected, multiplied, moved around, highlighted, and shaded. Features of a person are reconfigured into a portrait. Of course it is more accurate to say that features of a person may be reconfigured into multiple portraits. Because data is bounced around and repurposed, many different accounts may be rendered, accounts developed by many different actors with many different interests—journalists, campaigns, opposition candidates and campaigns, political parties, interest groups, regulators, etc.

As with the personal data elements required for donations in CFD and the highlighting and shading, rendering often draws on a normative landscape involving assumptions about human behavior and political processes. In the case of Proposition 8 in California, it would seem that data about donors supporting Proposition 8 were used with the assumption that donating to this cause was an affirmative act of resisting gay marriage.[114] The combination rendered donors as homophobic, anti-gay people who deserve scorn or even retaliation.[115]

Drawing on another situation involving contributions to Hillary Clinton's campaign to become the Democratic candidate for the U.S. President, data about donors was used to render Clinton a shady (if not corrupt) politician.[116] The rendering was produced by combining information about large contributions with the assumption that money is the prime influence on politicians.[117] Lessig explains that as First Lady, Clinton opposed a bankruptcy bill with provisions that were friendly to credit card companies, and she, presumably, convinced her husband to oppose it too.[118] President Clinton refused to sign the bill as passed in both houses of Congress, allowing it to fail in a pocket veto.[119] After she was elected as a senator from New York, Clinton seemingly switched her position, twice voting in favor of the bankruptcy measure,[120]

---

[114] *See* Second Amended Complaint, ProtectMarriage.com v. Bowen, 599 F. Supp. 2d 1197 (E.D. Cal. 2009) (No. 2:09-00058-MCE-DAD).

[115] *See id.*; David Lourie, *Rethinking Donor Disclosure After Proposition 8 Campaign*, 83 S. CAL. L. REV. 133, 148 (2009).

[116] *See, e.g.*, Cliff Montgomery, *Senator Clinton, House Democrats Sever Ties to Shady Donor*, AM. SPARK (Aug. 30, 2007), http://www.americanspark.com/2007/08-30-07_Dems-return-cash.html (stating that Hsu's "run-ins with the law . . . [were] beginning to be a public embarrassment").

[117] *See* Lawrence Lessig, *Against Transparency: The Perils of Openness in Government*, NEW REPUBLIC (Oct. 21, 2009 12:00 AM), http://www.tnr.com/article/books-and-arts/against-transparency.

[118] *Id.*

[119] *Id.*

[120] *Id.*

though ultimately opposing its final passage.[121] Critics decried this maneuvering, attributing Senator Clinton's change in stance to the $140,000 she had received in campaign contributions from the finance industry while running for office.[122] This narrative of Clinton's decisions to support and not support legislation is produced by presuming the power of money to influence. Of course, other assumptions could have been made. For example, in representing the state of New York, one might argue that she had a special *duty* to support the bill.[123] Instead, as Lessig notes, "Everyone learning the fact [of her funding] now 'knows' just why she switched, don't they? Whether true or not, money is the reason for the switch in this case."[124] In other words, the controversy over Hillary Clinton's change in position hinged on the fundamental assumption built into CFD—that money is the prime mover of politics.[125] Combined with this assumption, campaign finance data render candidates in a particular way.

Rendering might be thought of as the final step in CFD, so it is important to note that a rendering—an account of a person—can easily become the entry step of another run through the house of mirrors. Accounts of persons endure when posted on the Internet and at any point information in an account can be taken up for a new purpose, combined with other data, and used to produce a new rendering. Moreover, unlike the images of a real house of mirrors, the effects of CFD accounts are far from comic; they can be profound and enduring. There may, in fact, be no exit from this house of mirrors because the data persist, ever-ready for the production of new renderings.

IV. DISCUSSION/POLICY IMPLICATIONS

Practical obscurity, as described earlier, has been lost as a result of the electronic environment. CFD has been reconfigured from essentially a system of transparency holding candidates and campaigns accountable to practically a system that enables surveillance of donors. This can be seen in the case of the "donor lookup" feature found on OpenSecrets, a website of the Center for Responsive Politics.[126] The mission of the Center is a laudable one:

> The Center for Responsive Politics is the nation's premier research group tracking money in U.S. politics and its effect on elections and public policy. Nonpartisan, independent and nonprofit, the organization aims to create a more educated voter, an involved citizenry and a more transparent and responsive government. In short, the Center's mission is to:

---

[121] *Id.*
[122] *Id.*
[123] *Id.*
[124] *Id.*
[125] *Id.*
[126] *Donor Lookup: Find Individual and Soft Money Contributions*, CTR. FOR RESPONSIVE POLITICS, http://www.opensecrets.org/indivs/index.php (last visited Jan. 20, 2011).

> - Inform citizens about how money in politics affects their lives
> - Empower voters and activists by providing unbiased information
> - Advocate for a transparent and responsive government
>
> We pursue our mission largely through our award-winning website, OpenSecrets.org, which is the most comprehensive resource for federal campaign contributions, lobbying data and analysis available anywhere. And for other organizations and news media, the Center's exclusive data powers their online features tracking money in politics—counting cash to make change.[127]

No mention is made—no concern is expressed—about the importance of the First Amendment privacy interests in association and opinion formation, or of the long cherished value of the secret ballot, or of donors' lack of expectation that their information is broadcast to the world.[128] Instead, the assumption seems to be simply that information about donors will inform and empower. In other words, transparency is seen as an unqualified "good." But, as we have argued above, this is not the case.

The house of mirrors analysis shows that transparency is far from a simple matter, let alone an unqualified good. Transparency systems do not simply reveal "what is there" or merely put light on what otherwise takes place in the dark. Transparency involves "making" anew and creating new opportunities. An account of someone or some activity is produced, and the production—the rendering—is shaped by the medium in which the account is produced as well as a myriad of other factors, including the interpreted understanding of the activity being made transparent and tradeoffs between values. The medium and the normative landscape of assumptions and values in which transparency is produced must be taken into account in using transparency as a mechanism of accountability.

Acknowledging that transparency is a house of mirrors when implemented on the Internet is the first step to better balancing the tension between transparency and privacy in CFD. What are the next steps? What else does the house of mirrors metaphor tell us about how to better address and balance this tension in an electronic environment? In the house of mirrors metaphor, the question is: how can the mirrors be repositioned to achieve a desirable form of transparency without threatening the privacy of the voter? Is there a way to minimize the amount of light being focused on donors while at the same time keep the light appropriately focused on campaigns?

Lawrence Lessig argues that we should abandon the current system and adopt an entirely different model of campaign funding, one that is publicly financed and,

---

[127] *Our Mission: Inform, Empower & Advocate*, CTR. FOR RESPONSIVE POLITICS, http://www.opensecrets.org/about/index.php (last visited Jan. 20, 2010) (emphasis omitted).

[128] *See id.*

therefore, does not require information about donors or donations.[129] Daniel Solove, on the other hand, argues that some limitations on access and uses of public information may create "a workable compromise for the tension between transparency and privacy . . . ."[130] We agree in part with Solove but more is needed than limitations on access and use. To turn to public financing of campaigns or to merely change patterns of access and use is, in effect, to presume that the current setup is the only way CFD can be implemented on the Internet. This is not the case. Indeed, the house of mirrors analysis identifies a set of points at which the mirrors can be repositioned. Each of the aspects of the house of mirrors described above—entry, bouncing, highlighting, shading, and rendering—can be examined in terms of their role and effects on privacy and transparency. Each is a potential "lever point" for achieving a better balance of privacy and transparency in CFD (and by example in other cases).

In what follows we identify a set of possible strategies, but our aim is not to argue for a particular strategy—but only to identify the possibilities in light of our understanding of transparency and how it comes into tension with privacy in an electronic environment. Each of the processes in the house of mirrors constitutes a point at which some tinkering may redress the thrust towards transparency and afford more protection for privacy. Since this approach involves revisiting how transparency and privacy are constituted in CFD implementation on the Internet, the guiding principles must be the rationales for having transparency and for protecting privacy. In other words, we must keep in mind: 1) that privacy in forming opinions about candidates and campaigns should be unencumbered (there should be no fear of sanctions for engaging in speech that helps to understand candidates and campaigns) and the secrecy of the vote should be maintained; and 2) that campaigns and candidates should be held accountable for running campaigns that do not undermine democratic processes, and should be honest about who they are.

A. Entry

We begin our analysis with the entry into the CFD house of mirrors. At this point, information is collected. Currently, as noted above, CFD requires name, employer, occupation, home address, and the amount donated.[131]

There are at least two issues that need to be revisited here. The first is what items of information should be collected, and second, what information must be displayed

---

[129] Lessig, *supra* note 117, at 8. Somewhat similarly, Ian Ayres suggests that candidates establish a blind trust to fund their campaigns with donors contributing directly to the trust, and their donations remaining anonymous both to the public and to the campaign itself. Ian Ayres, *Disclosure versus Anonymity in Campaign Finance*, *in* DESIGNING DEMOCRATIC INSTITUTIONS 19, 19–54 (Ian Shapiro & Stephen Macedo eds., 2000). In this case, the reflection does not bounce to the campaign and elected officials cannot reward their patrons, removing the possibility of corruption. *Id.* at 28, 33.

[130] Solove, *supra* note 17, at 1195.

[131] 2 U.S.C. § 434(f) (2006).

in order to achieve the accountability aimed for by the system, and to retain a level of practical obscurity appropriate to the context.

The issue of what items are collected should be determined by the purpose or purposes to be achieved by the system. Some of the current data elements can be modified or eliminated without compromising the value of keeping candidates accountable. "Name" and "amount donated" would appear to be necessary for the system to operate but others are less critical. For example, "employer" is regarded as important because then the public can ascertain if several employees are contributing to a particular candidate, which may indicate that an employer has a special interest that could be promoted or furthered by the candidate. But one's occupation may not be necessary, as even if all college professors or doctors were to donate to a particular candidate the possible interest in the candidate would be so diffuse to be somewhat meaningless. "Home address" provides relevant information on whether a donor is eligible to vote for a candidate but provides more precise information than is needed. Instead, one's congressional district alone should suffice. Alternatively, entry to the CFD system could be designed as a two-step process where identifying information was altered in such a way that its meaning could be retained but not the specifics. This would entail developing anonymizing techniques that conveyed categories deemed relevant to CFD but not identifying information.

The question of what information should be displayed entails the balancing between transparency and privacy. Information about amount donated is currently displayed as the exact amount a donor gives, but for purposes of accountability as well as privacy, the amounts could be reported as ranges or categories, e.g., $1–$500, $1,000–$3,000, etc.[132] Similarly, one's full name need not be posted; instead, a first initial and last name may suffice for purposes of accountability as well as providing some privacy. This would mean in effect, the creation of a form of practical obscurity in that someone who wished to use the data for transparency or surveillance purposes would need to exert additional effort to determine who a donor actually is.

What we are suggesting here is that we revisit the decision about what data needs to be collected when a donation is made in light of the fact that the data will be posted on the Internet. Although arguments can be made for the value of collecting each item of information, it doesn't follow that all items have to be posted or posted in the form collected.

The five items currently collected are collected for multiple purposes and these purposes were not taken into account when the CFD system went on the Internet.[133] Some information seems to be collected to ensure that the donation comes from a legitimate donor, i.e., name and address.[134] Some information seems to be collected

---

[132] *Id.*

[133] *See* McGeveran, *supra* note 31, at 11–12 (explaining that "change in technology qualitatively transformed the nature of disclosure laws" such that "law[s] may remain the same, but [their] effect is entirely different").

[134] *See* Scott M. Noveck, *Campaign Finance Disclosure and the Legislative Process*, 47 HARV. J. ON LEGIS. 75, 100–01, 107 (2010).

because it reveals something relevant to appropriate/inappropriate influence, e.g., size of donation and employer.[135] The question that has to be raised here is which information is relevant for accountability, which to detect corruption, and which for citizens to evaluate the candidate. Perhaps some will argue that it is better to err on the side of making all information public rather than using a particular theory of corruption. On the other hand, information relevant for making sure the donor is a real person seems very different from information relevant to figure out influence.

B. Bouncing

The lever points in CFD are inextricably intertwined, so a change in entry information will automatically affect bouncing. If the information fields are modified, different information will be bounced around. Indeed, if one assumes that the Internet is free and open and uncontrollable (i.e., that bouncing is an inherent feature of the Internet), then the only way to control bouncing is to control the information posted. However, information posted on the Internet can be restricted even when it is publicly accessible. At least two possibilities are readily apparent. One is the use of the "read-only" format and the other is control of searching capabilities. A different balance of transparency and privacy (than we currently have) would be achieved by making CFD records posted on the Internet "read-only." The records would then be accessible from the FEC website to anyone who wanted to see them, but could not be easily downloaded or copied and pasted elsewhere.[136] To be sure, individuals and organizations could find ways to "get" and manipulate the information, but they could do so only with some difficulty, e.g., copying and re-entering, using special technological tools. The "read-only" status would produce (and reintroduce) some element of "practical obscurity."[137]

Another possibility is to manipulate or eliminate the search functions for CFD data. By using various tagging systems or regulating search engine companies, CFD data might be posted so that those searching for it would be directed primarily to the original FEC site. It could also be designed so that people would need to read through the data rather than automatically "finding" information of particular interest. In effect, "data mining" capabilities could be turned off or restricted. None of these technical measures would guarantee that CFD data would never be duplicated, re-presented, or mined. Rather these technical measures create a form of practical obscurity. In effect, they constrain bouncing by putting up hurdles.

Lawrence Lessig's insight in *Code and Other Laws of Cyberspace* is relevant here in that achieving a desirable balance of transparency and privacy is likely to involve

---

[135] McGeveran, *supra* note 31, at 29.

[136] *See id.* at 12 (discussing the current accessibility of information of the FEC website).

[137] *See supra* notes 6–7 and accompanying text.

some combination of law, architecture, norms, and markets.[138] The technical measures just mentioned—"read-only" documents and restricted searching functions—could be supported by legislation that penalized those who manipulated and mined CFD data.

C. Highlighting and Shading

Architectural changes in entry and bouncing change the architecture for highlighting and shading; if we bring in a normative landscape as a component of highlighting and shading, it will return us to entry and what theories about corruption and influence are at work in the choice of five items.

Just as changing the entry information automatically affects bouncing, changes in entry information and bouncing together affect highlighting and shading. Privacy protections at entry and bouncing will serve to restrict highlighting and shading. But more to protect donor privacy can also be done at this stage.

Highlighting and shading are the result of many factors but the starting place is generally a combination of repurposing and manipulation. Information about donors is mined for correlations.[139] The data are disaggregated and then re-aggregated and repackaged for purposes quite different than those for which they were collected. Remember that in the case of California's ballot initiative for Proposition 8, data collected in the name of the transparency of the campaign was combined with location data and then repurposed to targeting of donors.[140] Repurposing of data is constrained by the limitations mentioned under bouncing. But if the architecture of the system can be designed so that information fields are tied together, then it will be more difficult, if not practically impossible, to highlight and shade elements of the information. For example, if the possibilities for sorting of posted data are architecturally constrained, then again a hurdle is introduced that makes difficult for certain kinds of matching to occur. Another option is that data be displayed so that it cannot be combined with data in other systems because the system in which CFD is displayed is not interoperable with other systems. Again, this does not eliminate data matching but creates practical obscurity.

D. Rendering

In large measure, rendering is the outcome of the prior three processes. Changes in entry, bouncing, and highlighting/shading lead to changes in the kinds of accounts (of campaigns, candidates, and donors) that can be rendered. Rendering in unintended ways would be more difficult if the above protections are put in place.

---

[138] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 186–87 (1999) (discussing the need to strike a "balance between individual and collective rights . . . and the implicit regulations of the architectures of cyberspace").

[139] *See* McGeveran, *supra* note 31, at 12–13.

[140] *E.g.*, Noveck, *supra* note 134, at 99.

In addition, there are some measures that might be targeted specifically to make unintended rendering more practically difficult. For example, expunging campaign finance data after a limited period of time, say two years after an election, would constrain the possibility of long-term accounts of donors which are unnecessary for purposes of candidate and campaign accountability. For this to be effective, it might necessitate "self-destruct" codes built into the CFD data. The self-destruct code would transfer so that every time data is copied, the self-destruct code is automatically copied.

CONCLUSION

As mentioned at the beginning of the last section, our aim is not to argue for any particular change but rather to emphasize that there are a range of possibilities. Our aim is to open the black box of the current CFD system and show that it is not the only way it has to be.[141] In hindsight it seems that moving CFD records to the Internet might have been done (naively) under the (blind) assumption that "public records" must mean making all possible information available to everyone who is interested. Of course, this concept of "public records" is misleading if not inchoate. Selective data is collected. And, information posted is not simply posted; it is manipulated, mined, and interpreted. The selection of data is made on the basis of a set of purposes inseparable from ideas about what counts as corruption, how politicians may be influenced, what donors seek, and so on. Currently, posting data does not simply mean making it available to citizens; it means making it available to those who manipulate it and repost it for a variety of purposes. The reality of information posted on the Internet should be brought together with a new concept of what "public records" should mean. The new concept should take into account the nature of the Internet and the value of privacy alongside the value of transparency.

Most of the changes we have identified as a result of the house of mirrors analysis focus on the architectural components of CFD, the primary area of our concern. However, we recognize that for these changes to be effective, as well as for other complementary changes to be incorporated, a more complete analysis of how architecture works with law and social norms is necessary. In this case, that would entail, at the least, an investigation into the implementation practices of the Federal Election Commission and a fuller understanding of cultural and political theories of corruption.

---

[141] Langdon Winner, *Upon Opening the Black Box and Finding It Empty: Social Constructivism and the Philosophy of Technology*, 18 SCI., TECH. & HUM. VALUES 362, 365 (1993) (arguing that humanitarians and social science writers should not "look[ ] upon technological developments as black boxes" but instead "open[ ] the black box" as "social constructivists").