Deniable Payments and Electronic Campaign Finance

Matt Franklin
Xerox PARC
3333 Coyote Hill Road
Palo Alto, CA 94304
U.S.A
phone: (650) 812-4228
Email: franklin@parc.xerox.com

Tomas Sander
InterTrust STAR Lab
4750 Patrick Henry Drive
Santa Clara, CA 95054,
U.S.A.
Phone: +1 (408) 855 0242
Email: sander@intertrust.com

The success of political candidates in U.S. elections depends critically on the amount of money they can spend on their campaign. Candidates are heavily dependent on donations to raise the large sums of money that are needed to succeed. Candidates thus become vulnerable to influence buying by wealthy citizens, corporations, or Political Action Committees (i.e., groups that are able to raise and bundle significant amounts). Influence buying can range from simply buying time with the candidate, to buying the opportunity to express opinions on particular political issues, to outright quid pro quo corruption where political positions are traded for donations. Candidates may also extort donations from potential donors, by threatening them with punitive treatment or indifference. The potential for political corruption has led to regular attempts to reform the system of campaign finance. Mainstream proposals include mandated disclosure of campaign donations (to expose suspicious correlations between the candidate's positions and the donors' interests) and limits on the amount of donations.

Ayres and Bulow [AyBu] propose a more radical approach for disrupting the "market" for monetary influence. Donations of any amount would be allowed, but all donations would be anonymous. In other words, any donor can contribute any amount to any candidate's campaign, but must not be able to prove to the candidate that he made a donation. Since a true influence buyer has no more credibility than a fake influence claimer, potential influence buyers have no incentive to actually make a contribution. Furthermore a candidate who tries to extort donations has no way to verify that the extorted party in fact followed his blackmailing, so extorting donations no longer makes sense either. We refer the reader directly to [AyBu] for a more detailed discussion of "mandated donor anonymity" and its consequences, constitutionality, and political feasibility.

To implement their proposal, Ayres and Bulow offer only a trusted third party design called the "Blind Trust". All donations are made through the Blind Trust, which has a policy of never revealing the identity of the donors. This reliance on a trusted third party is unsatisfying. Moreover, if donations to the blind trust are made by check or other traditional payment mechanisms, then external paper trails and bank records could later be used by the donor to prove to a candidate that a certain donation was made.

We view this as a cryptographic problem. An electronic payment mechanism is deniable (or "receipt-free" or "incoercible") if the customer is unable to prove to anybody that he made a certain purchase. To the best of our knowledge, this is a new notion for payment schemes, although deniability has been studied in other cryptographic settings (e.g., protocols for secret ballot elections). In this talk, we will introduce the problem of deniable electronic payment mechanisms, and show how they can be applied to the mandated donor anonymity problem. Our proposal is practical, and improves on the Blind Trust of Ayres and Bulow in several critical aspects.

[AyBu] Ian Ayres and Jeremy Bulow, "The Donation Booth: Mandatory Donor Anonymity to Disrupt the Market for Political Influence", Stanford Law Review 1998.