

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
18 July 2002 (18.07.2002)

PCT

(10) International Publication Number
WO 02/056230 A3

(51) International Patent Classification⁷: G07C 13/00,
G06F 17/60

(21) International Application Number: PCT/US01/43962

(22) International Filing Date:
21 November 2001 (21.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/252,762 22 November 2000 (22.11.2000) US

(71) Applicant (for all designated States except US): VOTE-
HERE, INC. [US/US]; Suite 250, 3101 Northup Way,
Bellevue, WA 98004 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): NEFF, C., Andrew
[US/US]; 3048-164th Place N.E., Bellevue, WA 98008
(US). ADLER, James, M. [US/US]; 13220 N.E. 114th
Street, Redmond, WA 98052 (US). BERG, Andrew, C.
[US/US]; 12227 N.E. 136th Place, Kirkland, WA 98034

(US). HORNBAKER, John, H. III [US/US]; 411 Ward
Street, Seattle, WA 98109 (US). JANKE, Leonard, C.
[CA/US]; 10770 N.E. 29th Avenue, Apt. 188, Bellevue,
WA 98004 (US). BENTSON, Randolph, A. [US/US];
2322 - 37th Avenue, S.W., Seattle, WA 98120 (US). MC-
CANN, James, R., III [US/US]; 122 - 27th Avenue East,
Seattle, WA 98112 (US). PETERSON, Eric, A. [US/US];
24009 - 26th Drive S.E., Bothell, WA 98021 (US).

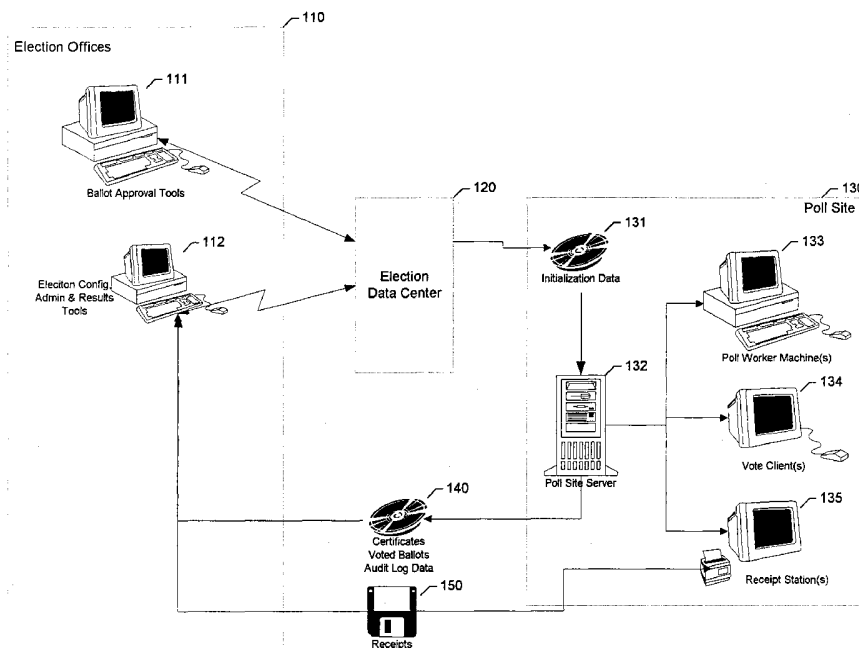
(74) Agents: LAWRENZ, Steven, D. et al.; Perkins Coie LLP,
P.O. Box 1247, Seattle, WA 98111-1247 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,
CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,
MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG,
SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN,
YU, ZA, ZW.

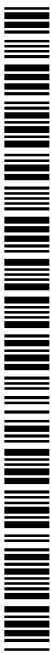
(84) Designated States (regional): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR,

[Continued on next page]

(54) Title: ELECTRONIC VOTING SYSTEM



(57) Abstract: A facility for conducting an election is described. The facility establishes a public key infrastructure for use in the election. The facility then employs the established key infrastructure in the operation of a voting site.



WO 02/056230 A3



GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent
(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR,
NE, SN, TD, TG).

(88) Date of publication of the international search report:
1 May 2003

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/43962

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07C13/00 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07C G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CRANOR AND CYTRON: "Sensus: A security-conscious Electronic Polling System for the Internet" IEEE, [Online] 31 January 1997 (1997-01-31), pages 1-9, XP002215651 Retrieved from the Internet: <URL:http://lorrie.cranor.org/pubs/hicss/hicss.html> [retrieved on 2002-09-30] the whole document	53-62, 67-93
X	HERSCHBERG: "Secure Electronic Voting Over the World Wide Web" MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 27 May 1997 (1997-05-27), pages 1-82, XP002215652 Massachusetts, USA page 22 -page 78	67-93

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

° Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

10 October 2002

Date of mailing of the international search report

10. 02. 03

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Lavin Liermo, J

INTERNATIONAL SEARCH REPORT

Inter application No
PCT/US 01/43962

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 92 03805 A (TECNOMEN OY) 5 March 1992 (1992-03-05) page 9 ---	42
X	BORRELL J ET AL: "An implementable secure voting scheme" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 15, no. 4, 1996, pages 327-338, XP004025182 ISSN: 0167-4048 the whole document ---	59-62
X	US 6 081 793 A (CHALLENGER DAVID C ET AL) 27 June 2000 (2000-06-27) column 3, line 10 -column 10, line 33; figures 1A,2A,9A,9E ---	16-41
A	CRANOR: "Electronic Voting" ACM, [Online] 6 May 1999 (1999-05-06), XP002215653 Retrieved from the Internet: <URL:http://web.archive.org/web/19990506040153/http://www1.acm.org/crossroads/xrds2-4/voting.html> [retrieved on 2002-09-30] the whole document ---	1,2
P,A	WO 01 22200 A (ADLER JIM ;GREEN RICHARD L (US); VOTEHERE INC (US)) 29 March 2001 (2001-03-29) figure 3 -----	1,2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 01/43962

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.
2. As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:
4. No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-2, 16-42, 53-62, 67-93

Remark on Protest

- The additional search fees were accompanied by the applicant's protest.
- No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-2, 16-42*, 53-62*, 67-93*

provide an alternative to the signatures and blinding signatures of the Sensus protocol, provide a decryption scheme requiring several entities, and implement a new cryptographical algorithm for a voting system.

* Claims 16-42, 53-62 and 67-93 do not fulfil the requirements of Article 33(2) (3) PCT (see documents in the Search Report considered as X-Documents and their references). These claims were therefore not declared as separate inventions, although their subject-matter differs from the subject-matter of claims 1-2.

2. Claims: 3-15

provide a new scheme for counting the votes allowing to detect uncounted votes

3. Claims: 43-52

provide an efficient storage for avoiding illegal accesses, which could correlate the voter with his ballot and this storage guaranting the privacy of the voter.

4. Claims: 63-66

provide a check of the valid formats of ballots allowable for the election

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No PCT/US 01/43962

Patent document cited in search report	A	Publication date	Patent family member(s)	Publication date
WO 9203805	A	05-03-1992	FI 904216 A WO 9203805 A1	28-02-1992 05-03-1992
US 6081793	A	27-06-2000	NONE	
WO 0122200	A	29-03-2001	AU 3770200 A AU 3922600 A WO 0120562 A2 WO 0122200 A2 AU 3922700 A EP 1224767 A2 WO 0120431 A2 US 2002078358 A1	17-04-2001 24-04-2001 22-03-2001 29-03-2001 17-04-2001 24-07-2002 22-03-2001 20-06-2002