CORE supplementary submission to NSW JSCEM

This submission is written by Vanessa Teague and Roland Wen. It has been endorsed by CORE's president.

We begin with some international and interstate electronic voting experiences, in answer to Mr Gareth Ward's question about what other jurisdictions are doing. This is not intended to be comprehensive, but does include both good and bad examples, and both Internet voting and computerised polling-place voting. The subsequent sections add comments on issues raised at the JSCEM hearing, including the possibility of open scrutiny of the code and whether any of the outstanding risks could have affected election integrity.

Many of the US examples are taken from a recent book, "Broken Ballots: Will your vote count?" by Barbara Simons and Doug Jones, available from University of Chicago Press and at http://brokenballots.com/ This book provides a rigorous and in-depth discussion of security and integrity issues associated with electronic voting. Although most of the examples are American, the security and integrity issues are of course universal. For example:

"Hackers, criminals, or countries can manipulate internet-based elections by inserting election-rigging malware into voters' computers. The Conficker worm, discovered in November 2008, illustrates the risk. Conficker rapidly infected between 9 and 15 million machines and has the capability of "calling home" for more instructions. In other words, the unknown creator of Conficker can instruct an infected machine to install additional malware remotely without the computer owner's knowledge. The new instructions could be targeted at specific candidates and elections, and fine tuned for each election."

The Conficker worm is an example of the modern trend of creating generic malware that can silently infect a very large number of computers over an extended period of time. The attacker has full control over these infected computers (commonly referred to as a 'botnet'), which can later be given instructions to mount specific attacks for any chosen purpose.

Another example of extremely sophisticated malware is the Stuxnet worm, which was apparently designed by a highly organised attacker for a specific task. Despite narrowly targeting specific machines, it propagated rapidly and was apparently undetected at its target until too late.

The following overview includes (non-US) International examples, US examples, and Australian examples of Internet and polling-place computerised voting. We emphasise the security, integrity, transparency and verifiability of the examples.

Non-US International examples

Estonia

Estonia has run Internet elections since 2005. In the most recent Estonian election, The Center Party, which was announced as coming second with 23% of the vote, filed a complaint in the Estonian Supreme Court requesting them to cancel the result of the elections because of alleged lack of secrecy, security and reliability of Internet voting. Their technical complaints are very similar to our criticisms of iVote, including the possibility of vote manipulation at the client machine that we described the last section of our first submission. Their complaint was dismissed because it was not filed in time; they announced plans to file a petition to the European Court of Justice.

The announced second-place holder in the election thus has a sound technical argument for rejecting the election outcome.

Source: The Organisation for security and cooperation in Europe (OSCE) report on the Estonian election: www.osce.org/odihr/77557

Norway

A good example of transparency, as described in our first submission. Arguably not a genuine example of verifiability, but the Norwegian authorities have a wealth of publicly available analysis of the issues.

Source: OSCE report: www.osce.org/odihr/88577

Switzerland

Switzerland has 3 different Internet voting projects, administered separately and quite differently by Geneva, Zurich and Neuchâtel. After many years of trials in less important elections, two of the systems were expanded in 2011 to federal elections and to other cantons.

Netherlands

An early adopter and early abolisher of electronic voting. Voting machines in polling places were discontinued when a group called "we don't trust voting computers" hacked the devices and demonstrated they could both manipulate votes and detect from a distance how people were voting.

Source: Bart Jacobs and Wolter Pieters, "Electronic Voting in the Netherlands: from early adoption to early abolishment" http://www.cs.ru.nl/B.Jacobs/PAPERS/E-votingHistory.pdf

Anne-Marie Oostveen, “Outsourcing Democracy: Losing Control of E-Voting in the Netherlands”. In: Policy & Internet 2.4 (2010), pp. 201– 220.

http://www.psocommons.org/policyandinternet/vol2/iss4/art8

Council of Europe Guidelines:

The Council of Europe publishes guidelines on electronic voting system transparency:

"Access to documentation including minutes, certification, testing and audit reports as well as detailed system's documentation explaining in details the operation of the system, is essential for domestic and international observers."

Source: The Council of Europe Directorate General of Democracy and Political Affairs "Guidelines on transparency of e-enabled elections" http://www.coe.int/t/dgap/goodgovernance/Activities/E-voting/E-voting%202010/Biennial_Nov_meeting/Guidelines_transparency_EN.pdf

US examples

The USA is a large and diverse country, in which electoral administration is very decentralised and a phenomenal variety of voting technologies have been tried.

Computers in a polling place

The debate on the security of computers in the polling place has mostly been settled by the adoption of a voter-verifiable paper record, usually in the form of a VVPAT or optical-scan paper ballot. (See verifiedvoting.org for a map of how many states require this.) Some illustrative examples are:

California

In 2007 the California Secretary of State commissioned a wide-ranging "top to bottom" technical review of voting systems. The researchers found numerous serious security vulnerabilities which could have allowed an attacker to manipulate votes. For example:

"The testers discovered numerous ways to overwrite the firmware of the Sequoia Edge system, ..., the attackers controlled the machine, and could manipulate the results of the election. No source code access was required or used for this attack, ..."

All direct-recording electronic voting machines in California now produce a voter-verifiable paper audit trail.

Source: http://www.sos.ca.gov/voting-systems/oversight/top-to-bottom-review.htm

Florida

In April 2012 an optical scan vote tallying system mistakenly awarded to seats to the wrong candidates in Palm Beach County, Florida. This was corrected after the paper ballots were audited. It is unclear how it could have been detected or corrected if there had been no paper record.
Source: Computerworld:
http://www.computerworld.com/s/article/9225816/E_voting_system_awards_election_to_wrong_candidates_in_Florida_village

Internet Voting

There is no straightforward method of achieving verifiability for Internet voting, because it's no use asking a voter to print their own "paper audit trail" at home. This is why most US computer scientists and electronic security experts oppose Internet voting - it has at least the same potential security vulnerabilities as computers in the polling place, and no human-readable paper audit trail.

Washington DC

In 2010 electoral officials in Washington DC ran a courageous experiment: they put up a practice version of their open-source Internet voting software and encouraged people to test it or attempt to hack it. This is the only example we know of in which attempts to hack the system were explicitly made legal, which allowed legitimate researchers to attempt to attack it and to publish their results. It's also a rare example of open-source Internet voting, though not an example of the long, open process of careful public and expert review that we advocate. The result was an insecure system, but by being open and transparent, the electoral officials were made aware of the vulnerabilities in time to call off the trial. The system would otherwise have been trusted for returning votes, while remaining vulnerable to outside attack.

Some quotes from the researchers who compromised the system:

"Within 48 hours of the system going live, we had gained near complete control of the election server. We successfully changed every vote and revealed almost every secret ballot. Election officials did not detect our intrusion for nearly two business days—and might have remained unaware for far longer had we not deliberately left a prominent clue."

They go on to say that they detected other attempted intrusions from Iran, India and China, which probably would have succeeded if the authors hadn't changed some passwords. They also asked electoral officials afterwards about the attack:

"They explained that they found our modifications to the application code ... although this required several days of analysis. They confirmed that they were unable to see our attacks in their intrusion detection system logs, that they were unable to detect our presence in the network equipment until after the trial, and that they did not discover the attack until they noticed our intentional calling card."

Source: "Attacking the Washington, D.C. Internet Voting System"

Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman

Proc. 16th Intl. Conference on Financial Cryptography and Data Security (FC '12)

https://jhalderm.com/pub/papers/dcvoting-fc12.pdf

Arizona

Internet voting was used in 2008 and 2010 for UOCAVA voters (Uniformed and Overseas Citizens Absentee Voting). This was an unusual system in which voters received a ballot which they printed, marked, scanned, and then uploaded from their own computer. Electoral officials in Arizona seem to have thought that the paper printout reduced the risks of Internet voting, but this is not really the case: problems of voter authentication, and of vote manipulation at either the voter's PC or the election server would probably have been similar to iVote. The paper trail would be infeasible to count, and voters had no evidence that their printout matched what they had actually submitted.

Helios

This is an end-to-end verifiable system that was developed by US cryptography researchers. It provides very strong evidence that it produces the correct tally, if the voters correctly perform a rather complicated protocol for casting their votes. Helios has never been used in political elections, but has been used for several professional societies and University elections.

See www.heliosvoting.org.

Further reading

Rather than list more US examples, we recommend two publications illustrating the US debate on Internet voting:

- The Election Assistance Commission's survey on Internet Voting, www.eac.gov/assets/1/Documents/SIV-FINAL.pdf
    - *This is a comprehensive survey of US and other electronic voting projects that used the Internet, including those that accepted votes from remote locations and those that sent votes over the Internet from controlled polling places. The list of acknowledgements on the first page includes various e-voting vendors and administrators, and no security or cryptography researchers we recognise. The survey is non-judgemental about security and integrity issues.*
- The National Institute of Standards (NIST) "Security Considerations from remote electronic UOCAVA Voting" www.nist.gov/itl/vote/upload/NISTIR-7700-feb2011.pdf
    - *This survey focuses on security issues, and concludes with three issues that "remain to be significant challenges." These are remote authentication of voters, the possibility of vote manipulation at the voter's computer, and the difficulty of verifying (which they call "auditing") the result.*

Australian examples

Most Australian electronic voting trials have been designed to improve access for vision impaired and other disabled voters, or for voters who have difficulty accessing postal voting. A voter can tell whether a system offers them a dignified and accessible voting option, but it's much harder to tell whether the whole system is private and secure. Our aim is to make sure security and integrity concerns are made explicit and accurately assessed, so that everyone can make a well-informed decision about which technology or people to trust to record their vote.

AEC trial of computers in a polling place (2007 Federal Election)

These computers produced a printout with a barcode representing the vote. Although it was not encrypted, it was also not possible for a human to read. This was specifically designed with the privacy of vision impaired voters in mind, so that they could ask for assistance with their printout without compromising privacy. This trial was discontinued because of cost. CORE supported the continuation of this project, though we recommended that if it was extended to voters who could read their own printout it should include a voter-verifiable printout.

AEC trial of remote electronic voting for Defence Force personnel (2007 Federal Election)

This software solution was provided by Everyone Counts, and included a receipt mechanism very similar to iVote's. Our submission to the federal JSCEM explained that this receipt mechanism did very little to prevent vote manipulation.

Current VEC project (proposed for Victorian state elections)

This is a polling-place system, which will be both transparent and verifiable. It will have openly-readable source code, and each voter will get a genuine proof, based on a paper record, that their vote was correctly recorded and correctly included in the count. It is possible there may also be an Internet voting system for people who require assistance to fill in a paper ballot and who would have difficulty attending a polling place.

AEC double-recorded telephone voting system (2010 Federal Election)

Although we did not suggest this system, and acknowledge that the user interface was far from ideal, it seems to have been designed with vote integrity in mind.

Proposed telephone-to-computer interface (proposed by Vision Australia and the AEC)

Unfortunately a telephone communicating with a computer recording the vote is if anything harder to secure than ordinary Internet voting. Nor is it necessarily private - if the voting data appear on the computer then someone with access to the computer could potentially discover the votes. Many of the manipulation and privacy attacks described for Internet voting apply to this scenario too, and some mitigations such as digital signatures and electoral-commission controlled encryption are impossible.

Some comments on matters that arose during the JSCEM hearing

Everyone Counts' Non-Disclosure Agreement

We have included the "Open Code Advantage Agreement NDA" with this submission, to illustrate that it would have prevented us from publishing freely on electronic voting. We

understand that private security firms generally return confidential reports to their clients, and would not be significantly hampered by this kind of agreement. We note that the reports commissioned by NSWEC to evaluate iVote's security remain secret. Hence there are some people (like us) who can say freely what we think of iVote, some others (like the security auditors) who have seen the source code and system details, and no-one in both groups.

Some notable quotes from the "Open Code Advantage Agreement":

"Expert shall not in any way ... analyze the Source Code or any other Confidential Information for the purposes of creating or which results in the creation or development of other computer programs, ... which compete with the eLect Platform"

This would have made it hard for us to work on the VEC project or our other research. Such clauses are fairly common in industry NDAs, but they impede independent expert evaluation of voting systems. Anyone who actually knows about voting systems will subsequently work on other voting systems.

"No Publicity. Without the prior written consent of Everyone Counts, Expert will not disclose to any person other than the Receiving Party ... any results of the evaluation of the Confidential Information."

This explicitly prevents us from making our findings public.

Previously the arrangement was that third parties given access to the source code and other confidential material were only required to have an NDA with the NSWEC, not Everyone Counts. However Everyone Counts changed its policy so that every individual is now required to also have a direct NDA with Everyone Counts. After the Clarence By-election, the attached NDA was newly created. The comment at the start of the NDA (dated 5/12/11) (written by the vendor, not by us) clearly states:

"The whole point of this Expert NDA is to bind the actual individial(s) [sic] accessing the Source Code to the binder of secrecy. If the Client hires a corporation to perform the evaluation, we would still need to have the actual individial(s) [sic] accessing the Source Code enter into this document."
For the proposed source code review, we objected to this NDA with Everyone Counts and we suggested that we should instead enter a standard government confidentiality agreement with the NSWEC. Both the NSWEC and Everyone Counts insisted that this was not an option.

This experience has significantly contributed to our belief that the only workable solution is completely open source code and documentation.

Our last sections add our comments to the detailed technical discussions from the JSCEM about the nature and extent of attacks on privacy and integrity.

Privacy and the iVote ID

Mr RADCLIFFE: Equally, if a person phoned us and said, "I did not cast a vote", we would be quite prepared to take a statement from them to that effect and nullify the vote that had been cast under that particular i-vote ID and re-enable them to cast another vote.

Mr ANDREW FRASER: Which basically means you could access someone's vote and know how and where they voted whereas under a paper system you cannot.

Mr RADCLIFFE: No, you could not. The actual preferences were encrypted through encryption keys that were locked away through a set of passwords held by a quorum of five or six members of an electoral board.

We believe Mr Fraser is correct. Although it is true, as Mr Radcliffe says, that the votes were encrypted with a key that was shared by five or six members of the board, there was a period beforehand when the votes were unencrypted on the server, along with their corresponding iVote number. This is detailed in our first submission, Section 2.4 "Vote Secrecy Issues."

Vote manipulation and the "man in the browser attack"

Mr RADCLIFFE: Not many. That was one instance where something was flagged to us. Another instance is the man in the browser attack that I outlined before where you could create a virus that would in theory undetectably change people's votes on their PC. But as I said, it would be very hard in practice for that to have any meaningful impact on an election. In this case again we assessed this and we were very aware of the fact that it could create a perception that you could vote twice, but we are also very confident that in fact it was not a real attack because no second vote was cast.

Although this was transcribed into one paragraph, Mr Radcliffe is talking about two different attacks. We have emphasised repeatedly the attack in which manipulation on a voter's PC would in practice undetectably change people's votes. This is detailed in our first submission, Section 7 "Vote tampering case study." We would be happy to provide a demonstration whenever the iVote practice server is re-enabled. He is referring to a different attack when he says, "In this case again we assessed this and we were very aware of the fact that it could create a perception that you could vote twice, but we are also very confident that in fact it was not a real attack..."

More on vote manipulation

Mr RADCLIFFE: Again, all of these potential issues are around a single vote. If you compare an example of protecting a single vote in the current paper system, it is far, far more difficult with all these attacks to have the impact of changing a single vote than any potential attack on the paper system.

Our point is that it could be much easier to change a large number of votes in an electronic system than a paper one.

Conclusion: Could any of the outstanding vulnerabilities have affected election integrity?

Did iVote have any outstanding vulnerabilities that could have impacted election integrity? This is possibly the most important question to answer before deciding whether iVote should be retained, scaled back, discontinued or expanded. Mr Brightwell said in his evidence that "We did not leave on the record any risk that we could see that had any substantial impact on the electoral process in the scale of the activity we were dealing with," but he was referring to a very specific set of risks identified in the "iVote Stratsec Test report - detailing actions taken and mitigation of risks identified during white and black box testing," which remains secret. Yet it is clear that there were risks, including the risk of voter impersonation and client-side vote manipulation. The only disagreements are about the extent to which they could have been exploited without detection and how they compare to analogous risks in alternative voting methods. We also know that anyone with administrator privileges on the server could have manipulated any of the votes without being detected by the receipt mechanism, though we do not know how difficult it would have been for either insiders or outside hackers to achieve such access. Without a clear understanding of what the risks were, how easy they were to exploit, and how they compared to the risks of alternative voting methods, it is impossible to make an informed decision on the future of iVote.

OPEN CODE ADVANTAGE
EXPERT NON-DISCLOSURE AGREEMENT

This Open Code Advantage Expert Non-Disclosure Agreement ("Agreement") is entered into on _____, 2011, between EVERYONE COUNTS INC., a Delaware corporation, with offices located at 4435 Eastgate Mall Suite 100, San Diego, California 92121 ("Everyone Counts"), and _____, an [individual/ entity] ("Expert").

Comment [e1]: The whole point of this Expert NDA is to bind the actual individual(s) accessing the Source Code to the binder of secrecy. If the Client hires a corporation to perform the evaluation, we would still need to have the actual individual(s) accessing the Source Code enter into this document. In that case the separate corporation would also need to sign this document (modified to make applicable to an entity rather than an individual by correcting the opening paragraph).

RECITALS

A. Everyone Counts provides election and voting technologies, including the eLect Platform solution suite;

B. Expert is [an employee/ a consultant] to [Name of Potential Customer] ("Receiving Party") and has been asked to assist Receiving Party in evaluating the eLect Platform source code as part of Receiving Party's evaluation of a potential or existing business relationship, as the case may be, with Everyone Counts ("Authorized Purpose");

C. Expert understands and acknowledges that the eLect Platform source code as well as other proprietary information as may be provided by Everyone Counts pursuant to the Authorized Purpose are all the confidential information of Everyone Counts; and

D. Everyone Counts is willing to disclose the eLect Platform source code and such other confidential information to Expert but only pursuant to the terms of this Agreement.

NOW, THEREFORE, in consideration of the mutual provisions contained herein, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Definitions

(a) "Confidential Information" means all confidential or proprietary information disclosed by Everyone Counts or otherwise learned by Expert or Receiving Party pursuant to the Authorized Purpose, including, but not limited to, the Source Code, inventions, ideas, processes, methods, copyrights, patents, techniques, formulas, computer programs, data, files, hardware, specifications, prototypes, designs, know-how, drawings, marketing plans, financial data, customer lists, referral and vendor sources, policies, and other procedures, and other information whether in digital, written, oral and/or physical/sample form.

(b) "Source Code" means the source code for the eLect Platform.

2. Scope of Review. Expert shall only review the Confidential Information only to the extent required for the Authorized Purpose, and for no other purpose. Everyone Counts is not obligated to disclose any information to Expert. Everyone Counts retains the sole and exclusive ownership and intellectual property rights to the Confidential Information, and no license or any other interest in the Confidential Information is granted to Expert. Expert shall have no rights of any nature whatsoever in or to the Source Code or the object code created when such source code is compiled. Expert acknowledges that all Confidential Information received from Everyone Counts is provided without any express or implied representation or warranty by Everyone Counts as to the accuracy or

completeness of such Confidential Information. Expert must immediately disclose any problems detected in the Confidential Information to Everyone Counts.

3. Restrictions. Expert agrees to use best efforts to protect the Confidential Information, but in all events will use at least a reasonable degree of care. In addition to such degree of care, Expert shall not in any way (a) use or permit the use of the Source Code or any other Confidential Information by any person; (b) copy or create derivative works of any portions of the Source Code or any other Confidential Information; (c) modify the Source Code or any other Confidential Information in any way; (d) distribute any enhancements, improvements or derivative works based upon Confidential Information; (e) copy, review or analyze the Source Code or any other Confidential Information for the purposes of creating or which results in the creation or development of other computer programs, or other tools, products or services, which are functionally, visually or otherwise identical or similar to the eLect Platform or which compete with the eLect Platform; (f) sell, license, transfer, lease, give away, distribute or otherwise dispose of the Source Code or any other Confidential Information; (g) disclose or otherwise transfer the Confidential Information to any third party at any time; (h) merge the Confidential Information with any other technology, formula or materials; and/or (i) remove any trademark, copyright, patent or mask work notices and/or other proprietary legends contained within any of the Confidential Information. To further protect Everyone Counts' interest in the Confidential Information, Expert agrees that Expert shall not in any way incorporate, use and/or exploit any part of the Confidential Information (disclosed separately or embodied in Everyone Counts' products, equipment or operations) in Expert's and/or any other party's products or businesses, including without limitation to develop, produce and/or distribute any products or services that derive from or use the Confidential Information. The provisions of this Section 3 shall survive the termination of this Agreement.

4. Legal Process Exception. Except for the Source Code, which shall always be deemed to be Confidential Information, the obligations and restrictions herein shall not apply to any other Confidential Information that is released pursuant to a court order or otherwise required by law (including without limitations as required under federal or state securities laws) provided that Expert immediately notifies Everyone Counts of such court order or legal requirement, and gives Everyone Counts a reasonable opportunity and cooperates with Everyone Counts to contest, limit or condition the scope of such required disclosure.

If Expert wishes to rely on the exceptions contained in subparagraph **Error! Reference source not found.** above, then Expert must demonstrate to Everyone Counts the facts underlying why the exception applies within thirty (30) days of receipt of the Confidential Information from Everyone Counts.

5. Unauthorized Use or Disclosure. Expert will notify Everyone Counts immediately upon discovery of any unauthorized use or disclosure of Confidential Information or any other breach of this Agreement and will reasonably cooperate with Everyone Counts to regain possession of the Confidential Information and prevent further unauthorized use and disclosure of the Confidential Information.

6. No Publicity. Without the prior written consent of Everyone Counts, Expert will not disclose to any person other than the Receiving Party (a) that the Confidential Information has been made available to the Receiving Party or Expert; (b) that discussions or negotiations are taking place

concerning a possible transaction between Everyone Counts and the Receiving Party; (c) any terms, conditions or other facts with respect to any such possible transaction, including the status thereof; or (d) any results of the evaluation of the Confidential Information.

7. Grant Back. The disclosure of Confidential Information pursuant to this Agreement is expressly conditional on the following. In the event that Expert makes or acquires any derivatives, enhancements or improvements to any aspect of the Source Code or any other Confidential Information, then as additional consideration for the disclosure of Confidential Information by Everyone Counts and other favorable provisions of this Agreement Expert hereby agrees to assign and hereby does assign and transfer to Everyone Counts all worldwide right, title and interest in and to such derivatives, enhancements or improvements to the Confidential Information, and to all modifications, enhancements and derivative works thereof, and to all intellectual property rights related thereto. Either during or following termination of this Agreement, Expert shall make any filings and execute any documents necessary for Everyone Counts to record, register, or otherwise perfect Everyone Counts' ownership rights in such derivatives, enhancements or improvements to any aspect of the Confidential Information.

8. Security.

(a) Expert shall maintain physical security procedures, acceptable to Everyone Counts, for information security related to the review of Confidential Information, including, but not limited to physical perimeter and access security for any location where the Confidential Information will be stored and reviewed.

(b) Expert shall maintain security procedures, acceptable to Everyone Counts, for systems and network security related to the review of Confidential Information, including, but not limited to: (a) installing firewalls at all perimeter connections for each device where the Confidential Information will be stored and reviewed; (b) installing intrusion detection software for each such device; (c) implementing all critical security-related software patches relating to products utilized in the storage of Confidential Information, including, but not limited to, the Source Code; (d) routinely monitoring the firewall, intrusion detection, system and router logs for anomalies; (e) implementing automated, real-time alerting by firewalls for suspected high-risk events that exhibit known attack signatures; and (f) using strongly encrypted media for all information storage.

(c) Expert shall maintain procedures, acceptable to Everyone Counts, with respect to servers and workstations security related to the review of Confidential Information, including, but not limited to: (a) hardening, to include disabling unused services; (b) configuring to resist installation of malicious code including viruses, sniffers, remote host-domination programs, and unauthorized process monitors; (c) configuring to resist unauthorized elevation of user privileges: (d) installing and maintaining anti-virus detection software; (e) routinely monitoring system and application logs for anomalies; and (f) using strongly encrypted media for all information storage.

(d) All Confidential Information, including, but not limited to, the Source Code shall not be transmitted outside of the servers meeting the security and other procedures set forth above. Confidential Information will only be delivered and returned on portable media using encryption methodology approved in advance by Everyone Counts.

9. Enforcement. The parties agree that Everyone Counts will be irreparably harmed and money damages will be inadequate compensation in the event Expert breaches any provision of this Agreement. The parties also agree that all the provisions of this Agreement shall be specifically enforceable against Expert by injunctive and other relief. The provisions of this Section 9 shall survive the termination of this Agreement.

10. Expert's Indemnity. Expert shall indemnify, defend and hold harmless Everyone Counts against all damages, claims, liabilities, losses and other expenses, including without limitation reasonable attorneys' fees and costs, whether or not a lawsuit or other proceeding is filed, that arise out of any violation of the provisions of this Agreement by Expert. The foregoing indemnity shall be payment obligations and not merely reimbursement obligations, it being understood that Everyone Counts and Expert have a "contrary intention" with respect to the provisions of paragraph 2 of Section 2778 of the California Civil Code. All rights and remedies conferred herein shall be cumulative and in addition to all of the rights and remedies available to each Party at law, equity or otherwise. The provisions of this Section 10 shall survive the termination of this Agreement.

11. Return of Materials. Expert will return all materials containing or constituting Confidential Information, together with any copies thereof, promptly after the completion of the Authorized Purpose, or upon the request of Everyone Counts. Additionally, upon request of Everyone Counts, Expert will destroy materials received or prepared by Expert that contain Confidential Information. Within ten (10) days after the request of the Everyone Counts, the Expert shall certify in writing that all Confidential Information has been so returned or destroyed and that the Expert has not retained any extracts or other reproductions in whole or in part, mechanical or electronic, of such material. Notwithstanding the return or destruction of the Confidential Information or the termination of this Agreement for any reason, Expert shall continue to be bound by Expert's obligations of confidentiality hereunder.

12. Export Compliance Assurance. Expert acknowledges that all products, software, and technology (herein referred to as "Products") obtained from Everyone Counts are subject to the United States (U.S.) government export control and economic sanctions laws. The Expert agrees that Expert will not directly or indirectly export, re-export, transfer, or release, (herein referred to as "export"), any such Products or any direct product thereof to any destination, person, entity, or end-use prohibited or restricted under such laws without prior U.S. government authorization as applicable, either in writing or as permitted by applicable regulation.

13. Governing Law/Venue. This Agreement shall be interpreted and enforced according to the substantive laws of the State of California without application of its conflicts or choice of law rules. Both parties irrevocably submit to the jurisdiction of the state and/or Federal courts in San Diego County, California for any action or proceeding regarding this Agreement.

14. Entire Agreement. This Agreement constitutes the entire agreement between the parties regarding the subject matter hereof and superseded all prior or contemporaneous understandings, oral or written. This Agreement can only be amended by a writing signed by both parties.

15. Notice. Any notice or other communication made or given by either party in connection with this Agreement shall be sent via facsimile (with confirmation) or by registered or certified mail,

postage prepaid, return receipt requested, or by courier service addressed to the other party at such other party's address set forth below:

EVERYONE COUNTS INC.	_____
4435 Eastgate Mall #100	_____
San Diego, California 92121	_____
Attn: Rick Forry	Attn:_____
Fax: (858) 876-1606	Fax:_____

16. Survivability. Expert agrees that all of Expert's obligations undertaken herein as the receiving party of Confidential Information shall survive and continue after any termination of this Agreement.

17. Severability. If any provision of this Agreement is held to be invalid, void or unenforceable, all other provisions shall remain valid and be enforced and construed as if such invalid provision were never a part of this Agreement.

18. Binding Effect and Assignment. This Agreement shall be binding upon and shall inure to the benefit of the parties hereto and their respective legal representatives, successors and permitted assigns. Expert may not assign Expert's rights hereto, or obligations hereunder, whether in whole or in part, or whether by operation of law or otherwise.

19. Validity. If any provision hereof is found by a court of competent jurisdiction to be invalid, void or unenforceable, the remaining provisions shall remain in full force and effect, and the affected provisions shall be revised so as to reflect the original intent of the parties hereunder to the maximum extent permitted by applicable law.

20. Attorney's Fees. In the event a dispute arises regarding this Agreement, the prevailing party shall be entitled to recover reasonable attorney's fees and costs in addition to any other relief to which such party is entitled.

21. Waiver. The failure to enforce any provisions of this Agreement shall not be deemed a waiver or a continuing waiver of the same or other provision of this Agreement unless such waiver is in writing and signed by the party to be charged.

22. Counterparts. This Agreement may be executed in several counterparts that together shall constitute one and the same instrument.

IN WITNESS WHEREOF, the parties have executed this Agreement on the date first written above.

EVERYONE COUNTS INC.

By:_____ _____

Name:_____ Name:_____

Title:_____

101730148.2