Teresa Hommel has worked with computers since 1967. Her voting machine simulation "Fraudo, the Fraudulent Voting Machine" at www. WheresThePaper.org has been used internationally to help people understand the security problems with computers used in voting.

Oversight Hearing: The Promises and Perils of Internet Voting
New York City Council
Committee on Technology and Committee on Governmental Operations
Wednesday, December 18, 2013, 10:00 AM
16th Floor Committee Room, 250 Broadway, New York, NY

Internet Voting is Vulnerable to Undetectable Fraud and Prevents Citizen Oversight of Election Procedures

Teresa Hommel, www.wheresthepaper.org

Thank you for allowing me to present testimony at this important hearing.

The New York City Council has provided leadership in the past to ensure that citizens could participate and observe our election procedures, and could participate in the selection of the voting equipment we now use.

Resolution 228-A of 2006 urged the New York City Board of Elections to conduct public testing of all voting equipment before purchase. Introduced by Robert Jackson, it passed unanimously on August 16, 2006.

Resolution 131-A of 2007 urged the New York City Board of Elections to select paper ballots and optical scanners as our city's new voting technology, rather than unauditable touchscreen voting machines. Introduced by Charles Barron, it passed unanimously on March 14, 2007.

I urge you now to reject the idea of internet voting because it is vulnerable to undetectable fraud, and because it would prevent oversight of election procedures by election administrators as well as citizens.

I urge you now to reject the idea that democracy is strengthened by convenience rather than by citizen participation in oversight of our government, and to find ways to strengthen civics education in our city to increase both citizen participation in oversight and voter turnout.

1. Representative government and the role of "we the people"

In a representative democracy, the government needs to do its work in public, and the people need to show up and observe and give guidance. Government behind closed doors is easily corrupted. Our government needs to not only be honest, but to do its work in public so that people can fulfill their role of oversight.

2. What's wrong with internet voting?

2.a. Internet voting prevents voters from witnessing their own votes being recorded and cast. Voters can't know if what they see on their computer screen at home is the same as what is

transmitted over the internet and received at the Board of Election's computers.

2.b. Election observers, election administrators, and candidates can't witness the storage, handling, and counting of votes. No one can know whether the tallies are accurate. Were the winners selected by the voters, or by innocent computer errors, or by some geek hacker kid down the street or anywhere in the world?

2.c. Internet voting would prevent our election administrators from performing computer audits to verify correct computer function. This is because we use secret ballots without tracking numbers, and tracking numbers are the basis for auditing when computers work with "online transactions."

With our current paper ballots and scanners, voters create an authentic first-hand record of their votes on paper. Although the votes are detected and counted inside a scanner, which is a computer, we perform audits with the paper ballots to verify that votes were read accurately, and credited to the intended candidate, and tallied accurately.

2.d. Some people say they "trust computers" and "trust their election administrators." But trust and trustworthiness are not the only considerations. If we want to live in a democracy, we need observable governmental procedures and citizen observers.

3. What if the computers were perfect?

With perfect computers, internet voting would still be inappropriate because it prevents government from conducting its business in public and prevents people from exercising oversight. And in reality, no computer connected to the internet is secure.

One of the largest computer crime surveys ever conducted--the FBI Computer Crime Survey of 2005 [www.WheresThePaper.org/FBI_ComputerCrimeSurveyPR.pdf]--reported that 87% of organizations were aware that they had had security incidents in one year, with 20% having 20 or more incidents. 64% of organizations lost money, showing that the incidents were serious, not trivial. 44% had incidents perpetrated by their own insiders.

If the FBI statistics hold true for election boards, then the more we transfer the work of elections to computers, the more uncertainty we will have about our election results. The FBI's survey showed that even companies that know the most about security--much more than ANY board of elections--still can't protect their own money. It means that computers are inappropriate for use in elections because they introduce unmanageable risks and vulnerabilities.

Running elections is a big job already, and it is unrealistic to expect our election boards to take on a second big job--to run secure computers--when the FBI survey showed that our most knowledgeable corporations can't achieve that.

4. What makes good elections? What is the citizen's role?

Our democracy is suffering from a continuing, subtle shift in our ideas about what makes good elections and what is the citizen's role.

• We have gone from "get it right on election night" to "if the tallies are potentially verifiable we don't need actual verification."

• We have gone from knowing that observers are the only way to get honest elections, to believing that it is more important to use computers because they are modern and convenient.

• We have gone from knowing that citizens have to show up in person and exercise meaningful oversight of government, to thinking that watching election returns on TV at home is good enough if you "trust" your election administrators.

• We have gone from knowing that democracy requires an engaged, informed citizenry, to NOT teaching civics in all our schools. We loudly urge people to vote but don't even whisper that voting is not the only obligation of citizens, and that voting alone cannot sustain democracy.

Our good government groups all want to "get out the vote." None of them is looking at what happens to the votes once cast, the fact that citizen oversight of vote-handling and election procedures is impossible with internet voting, and the fact that our election administrators cannot run secure elections with computers without a voter-marked paper ballot and proper audits after each election.

5. "Voter confidence" is a delicate "problem."

Telling people that unaudited and unauditable electronic voting and internet voting are scams might discourage voting, but it might stimulate enough outrage to increase other forms of citizen participation. Really, if we don't educate people and restore the people's role so we can have a "government by the people," we will reduce our elections to a ceremonial ritual. The ritual of elections, in and of itself, does not make a democracy. We know this from various dictators:

> Josef Stalin: "It's not who votes that counts, it's who counts the votes!"
> Anastasio Samoza of Nicaragua: "You won the vote, but I won the count."
> Boss Tweed of New York: "As long as I count the votes, what are you going to do about it?"

6. The New York City Council can take action to revitalize our democracy.

I urge the New York City Council to take action in the following areas to improve the participation of our people in all forms of involvement with our government, and in our elections.

a. Require all our schools to teach age-appropriate civics starting in kindergarten, so that our people understand our governmental infrastructure and the citizen's role in oversight.

b. Require all our schools to teach the skills for lifelong, sustained involvement with our government, so that individuals are knowledgeable and feel comfortable about staying informed, getting involved, and showing up and speaking in the offices and hearing rooms of our government.

c. Require our media to provide impartial, unbiased, and full reporting of news related to our governmental policies and actions.

When people are informed and have a relationship with their own government, we will not have to remind them to show up to vote in our elections.

Thank you.

New York City Campaign Finance Board

40 Rector Street, 7th Floor, New York, NY 10006
tel. 212.306.7100 fax 212.306.7143
www.nyccfb.info info@nyccfb.info

Testimony of Eric Friedman
Director of External Affairs, New York City Campaign Finance Board
City Council Committees on Government Operations and Technology
December 18, 2013

Good morning, Chairs Cabrera and Brewer. My name is Eric Friedman, Director of External Affairs for the New York City Campaign Finance Board. Thank you for the opportunity to testify today.

Fewer than 24 percent of registered Democrats voted in the September primary. In November, for the fourth consecutive election, voter turnout hit a new all-time low for a general mayoral election in New York City; barely 25 percent of all registered voters cast a ballot. To address this downward trend, our voting system must be modernized.

Today's consumer technology has made access to the Internet widely—though not universally—available. According to surveys conducted by the Pew Research Center, 85 percent of American adults (over 18) use the Internet[1]; 57 percent of American adults use a cell phone to go online.[2] Many of us go online to research and read news, purchase goods or services, connect with colleagues and friends, or manage our personal finances.

In an ideal world, our voting system would allow New Yorkers to connect with government and participate in the democratic process with the same ease and convenience they have come to expect in their everyday lives.

A system that allows voters to cast their ballot from a remote location, using any device with an Internet connection, is sometimes discussed as a cure to low voter turnout. Make voting easier and more convenient, the thinking goes, and more people will do it. It could be a money-saver as well; holding elections by Internet would reduce or eliminate the cost of administering poll sites, as well as printed ballots.

---

[1] http://www.pewinternet.org/Reports/2013/Non-internet-users/Summary-of-Findings.aspx
[2] http://www.pewinternet.org/Reports/2013/Cell-Internet/Summary-of-Findings.aspx

But serious challenges remain to be addressed before any reliable, broadly-used system of Internet-based voting is ready for adoption.

In a conventional system, a handful of ballots may be compromised through fraud, but an online, networked voting system may be vulnerable to more widespread manipulation. There are multiple entrance points for mischief: malware on the voter's personal computer could subvert the voter's intent without his or her knowledge; ballots could be intercepted in transit over the public Internet; servers or back-end systems controlled by election administrators could be compromised by remote attacks.

In 2010, the District of Columbia Board of Elections and Ethics conducted a test, inviting hackers to find vulnerabilities in a system they created as a pilot program for military and overseas voters to cast their ballots online. A team from the University of Michigan broke into the system within 36 hours, found a document containing every voter's name and password, and changed the voting results.[3] A subsequent report from the National Institute of Standards and Technology stated that ensuring the integrity of remote electronic voting "remains a challenging problem, with no current or proposed technologies offering a viable solution."[4]

It may be more difficult to preserve the secrecy of ballots cast over the Internet. Our current system requires that we authenticate each voter's eligibility to cast a ballot and guarantee the voter's privacy. In a system of online voting, these imperatives may contradict each other. An October 2013 report on Internet voting commissioned by the province of British Columbia, Canada notes that unlike in-person voting, "the connection between the voter's identity and the content of the ballot cast electronically is fundamentally and necessarily linked for both technological and policy reasons."[5]

Lastly, the lack of access to high-speed Internet in many communities represents a real concern. Nationwide statistics show that lower-income communities do not have the same access to broadband Internet at home as their better-off neighbors, and computers in libraries or work environments may not be private. Certain New Yorkers may simply not have equal access to the potential benefits of an Internet voting system.

Currently, none of the 50 states provide Internet-based voting for the general public. Thirty-two states (and the District of Columbia) allow voters serving in the armed services or living abroad to return voted absentee ballots electronically, via email or

---

[3] http://www.nytimes.com/2010/10/09/us/politics/09vote.html

[4] http://www.nist.gov/itl/vote/upload/NISTIR-7770-feb2011.doc

[5] http://internetvotingpanelca.blob.core.windows.net/internetvotingpanelca/ipiv-prelim-rpt-20131023.pdf

through a web portal, under limited circumstances.[6] For instance, Missouri allows only military voters serving in a "hostile fire area" to return ballots via email or fax. In the wake of Superstorm Sandy, New Jersey allowed some voters to email their ballots, an experiment that at least one official described as a "catastrophe" due to overwhelming demand.[7]

New York State does not allow citizens serving abroad to return their ballots electronically. If we are to move forward in this area, we should consider changes to State Election Law that would allow administrators to explore Internet voting for the narrow purpose of helping more New Yorkers abroad or serving in the military to cast valid, timely votes, if the challenges described above can be addressed.

There are several ways, however, that available technology can improve the in-person voting experience in New York right now, in significant and measurable ways.

- All New Yorkers should be able to register to vote and update their information online. The state has done a useful and important thing by establishing electronic voter registration through the Department of Motor Vehicles—but only for New Yorkers who possess a state ID. Allowing all voters to register and update their records online will help ensure New Yorkers who change addresses receive the information they need to stay engaged.

- We can also create smart, linked databases that automatically share information between government agencies and ensure the voter rolls are kept up to date. The Voter Empowerment Act, sponsored in the state legislature by Assemblyman Brian Kavanagh and Senator Michael Gianaris, would accomplish some of these important objectives.

- We have been voting with electronic ballot scanners for three years, but we still use ballots that are designed with the mechanical lever machines in mind. We should have ballots reflect the best practices of modern design. The Board of Elections is making efforts to increase the font size, but Assemblyman Kavanagh's Voter Friendly Ballot Act would do even more to make ballots easier to read and use.

- We can continue making voter information available in more convenient and accessible ways. The New York City Board of Elections made poll site locations

[6] http://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx
[7] http://usnews.nbcnews.com/_news/2012/11/06/14974588-new-jerseys-email-voting-suffers-major-glitches-deadline-extended-to-friday?lite

and sample ballots available through their website and a mobile app. Our own NYC Votes app provided information about candidates and poll site locations to thousands of New Yorkers during this election season. Our Voter Guide, in print, in video, and online gave every registered voter access to comprehensive, nonpartisan information about the candidates and the voting process.

- We can make better use of technology to collect data about activity at the poll sites, and learn more about voters' experiences. Collecting better data across the entire system in real time would ensure problems at the poll sites are addressed more quickly and efficiently, and help optimize the allocation of resources on Election Day. We will also be soliciting voter feedback through our own online survey, which will provide information that can help improve the voter experience.

- Jurisdictions in at least 27 states use some form of electronic pollbooks, according to research by the Brennan Center for Justice.[8] They can streamline check-in at poll sites. If they are linked to the statewide voter registration database, they can be used to determine a voter's correct address, and correct or update voter registration records at the polls—making affidavit ballots practically obsolete.

The technology to make these improvements is available now. Each would make voting quicker and easier, could save us money, and improve the health of our democracy. For these reasons and many others, State Election Law must be overhauled to provide administrators more flexibility, and more fully reflect the ways technology has evolved since the bulk of the law was written in the 1970's.

Thank you for the opportunity to testify today.

[8] http://www.brennancenter.org/analysis/testimony-presidential-voting-commission-can-modernize-elections

THE LEAGUE OF WOMEN VOTERS OF THE CITY OF NEW YORK
4 WEST 43rd STREET, SUITE 615, NEW YORK, NY 10036
PHONE: (212) 725-3541 • FAX: (212) 725-3443
WWW.LWVNYC.ORG • OFFICE@LWVNYC.ORG

Testimony to the New York City Council Committee on Technology, jointly with the Committee on Governmental Operations, RE: The Promises and Perils of Internet Voting Wednesday, December 18, 2013

Good morning. My name is Kate Doran. I serve on the Board of the League of Women Voters of the City of New York. As a multi-issue, non-partisan political organization we encourage informed and active citizen participation in government, work to increase understanding of major policy issues, and influence public policy through advocacy and education.

For over 90 years, voter education, voter service, and reform of election administration have been priorities for the League of Women Voters in New York. Accordingly we appreciate this opportunity to comment today.

Internet voting may be an ideal to which we aspire because of convenience, and because much of how we interface with government is trending paperless.
We however, are not confident that there is an Internet system secure enough at this time to merit extensive and expensive appropriation of city funds and other resources.

What we have now is a voting system which, when well administered is accurate, reliable and secure. We believe that our city resources should be concentrated on improving the administration of our paper ballot, optical scan system.

The NYC Board of Elections should be more proactive in seeking out technologies that could support the system we currently use. One example is to investigate printing ballots on demand. Voters are unified in their desire for a clearer more legible ballot. Tiny fonts are necessary, says the Board, because they must print a single ballot style in all the covered languages. Ballots on demand would solve this problem. Some have suggested that the Board print a two-language ballot. The Board contends that a two-language ballot would be difficult for poll workers to manage. With ballots on demand, poll workers would need only to know each voter's language preference. Printing ballots on demand would also mean that necessary changes to a ballot could happen much closer to the day of an election event. We urge the Council to ask the Board for a report comparing the costs and relative advantages of printing ballots in advance, versus purchasing technology for printing ballots on demand.

The ES&S DS-200 machine is, we understand, capable of handling ranked choice, or Instant Runoff Voting. Here is another example of a place where we believe the NYC Board of Elections should be taking the initiative, and we hope that the Council will nudge them along. New York State Board of Elections Co-Chair, Douglas A. Kellner,

recently made a presentation to the NYC Board in which he said, "The New York City Board of Elections can administer ranked choice voting. We use the ES&S DS-200 optical scanners to count ballots cast at poll sites. The DS-200 machines use the Unity 5.0.0.2 software. Both the hardware and the software are capable of formatting and recording ballots that use rank choice voting. The New York City Board of Elections would only need to develop a program to apply the statutory algorithm to determine the final results – not a particularly difficult or expensive process." We urge you in the Council to encourage the City Board of Elections to develop such a program, and to offer any assistance that is within your power and authority.

The League of Women Voters is not ready to support Internet Voting. We do however strongly support Online Voter Registration and Election Day registration. Paperless registration is more accurate, more secure, and cheaper. We are pleased that the Department of Motor Vehicles has enhanced opportunities for online voter registration, and we have learned that the New York State Health Care Exchange has created voter registration opportunities on their website.
We suggest that you ask the NYC Board of Elections to report to you about its goals and strategies for achieving greater numbers of online registrations.

The New York State League of Women Voters supports Early Voting. We in the City League understand that for the NYC Board of Elections, Early Voting would impose significant additional burdens in jurisdictions where election administration is already quite complex and challenging. We believe that for Early Voting to succeed we must seriously consider Electronic Poll Books. Ideally Electronic Poll Books would provide real time information as to when and where a voter has cast a ballot. Leaving aside Early Voting, Electronic Poll Books could be the next evolution in poll site registration lists, since the Board started to photocopy voters' signatures. The current registration books frequently print incorrect signatures, and sometimes show no signature at all. These voters, justifiably frustrated, have to vote by affidavit ballot, or get a court order to vote using a poll site scanner.

Redesigning poll worker training, and changing the deployment of poll site staff must accompany technological changes to election administration. We have testified several times in the past on the topic of training, and have put forth a model that would produce better outcomes, and could be Internet based.

E-mail communication can play a very important role as a less expensive way to deliver important, and perhaps last minute notices to voters. We congratulate the State and City Boards of Election for their agreement, and decision to include a field for voters' e-mail address on the "paper" voter registration form. We hope that the Board will use this information efficiently. But we think it shouldn't stop there. With political will and dedication, New York City can be a leader and a model in technological advances in election administration while still keeping our secure, auditable, paper based system.

We thank the Technology Committee for its interest in voting. And we thank the Governmental Operations Committee for its long and tireless leadership – especially Gale Brewer, who with her unique skill set, and persistence has made a real difference. The Board of Elections is a changed and better place owing to her oversight. As ever, we stand ready to work with you in support of our city and its voters.

susan@verifiedvotings.org
9177968782

Testimony of Susan Greenhalgh
Verified Voting Foundation

Before the New York City Council
Committee on Technology
Committee on Government Operations

The Promises and Perils of Internet Voting
December 18, 2013

I'd like to thank the Committees for the opportunity to testify today. Verified Voting is a national organization committed to safeguarding democracy in the digital age. Some of the most esteemed and prestigious computer security experts in the world serve on our board of directors and board of advisors and we are privileged to receive guidance on voting technology security from these computer scientists. These boards include Drs. David Jefferson, Barbara Simons and Avi Rubin, all of whom were asked by the U.S. Department of Defense to do a security evaluation of an Internet voting system developed for military voters by the Department of Defense in 2004. The resulting report[1] warned that the system could not guarantee the legitimacy of the votes and the DoD subsequently cancelled this online voting project stating the risks identified constituted a national security risk.

The assessment warned that the problem was not inadequate security tools or poor design. The researchers stated:

> *"We do not believe that a differently constituted project could do any better job than the current team. The real barrier to success is not a lack of vision, skill, resources, or dedication; it is the fact that, given the current Internet and PC security technology, and the goal of a secure, all-electronic remote voting system, the [DOD] has taken on an essentially impossible task. There really is no good way to build such a voting system without a radical change in overall architecture of the Internet and the PC, or some unforeseen security breakthrough."*[2]

Since 2004 there has been no radical change in the architecture of the Internet or some unforeseen security breakthrough. Instead the stealth and sophistication of computer attacks has only increased with the rise of state-sponsored computer attacks making the cyber world less secure now than it ever was. Earlier this year the former National Intelligence Director publicly stated that the U.S. is losing the cyber war.[3]

But while the security challenges of online voting remain unsolved, the interest in online voting from election officials and the public has been growing, driven largely by misconceptions and

---

[1] http://www.servesecurityreport.org/
[2] *Ibid.*
[3] Salant, Jonathan, "U.S. Losing Cyber War, Ex-Intel Chief tells BGov Conference," *Bloomberg,* Oct. 30, 2013

misinformation regarding Internet voting and I would like the opportunity to address some of these misconceptions now.

Misconception: Commercially available Internet voting systems are impenetrably, or absolutely secure and the systems in use have not been hacked.
Vendors have made claims that their systems cannot be hacked but none of these systems have been subject to publicly reviewable tests, "white-hat" attacks – in which hackers are asked to probe a system to identify vulnerabilities- or any type of government certification. Security claims are backed solely by the vendors' promises and are completely unsubstantiated. More importantly, there is no way to know if these systems have been infiltrated and compromised. Skilled hackers are able to breach systems and erase any trace of their actions. It has been estimated that most hacks are not detected for more than a year. Just because states that are allowing online voting have not identified any cyber attacks, that doesn't prove these system were not hacked.

Misconception: Sending ballots by email or fax is not Internet voting and does not have security risks.
There is a common misunderstanding that transmitting voted ballots by email or digital fax, then printing and scanning the ballot at the elections office is not Internet voting and does not carry with it the security risks that are identified with Internet voting. This is completely untrue. The risks associated with online voting exist whenever the marked, voted ballot is transmitted over the Internet and exposed to attack, deletion or tampering by hackers. While it may seem difficult to laypersons, setting up a program to intercept and filter out ballots sent to an elections office is not difficult for moderately skilled hackers, even if the ballots are encrypted. These ballots could then be deleted, manipulated or replaced without the voter's or election officials' knowledge.

Misconception: Internet voting systems in use today have been "approved" by the Department of Defense.
Vendors have boasted that their systems have been purchased by the Department of Defense. The implication is that the Department of Defense endorsed use of these systems for online voting. This is inaccurate. The Department of Defense has purchased some of these systems to deliver blank ballots online only, but <u>not to transmit (return) the voted ballots</u>. The federal government did not intend these systems to be used to transmit voted ballots over the Internet because of the unsolved security risks. [4]

Misconception: Internet voting systems travel over the secure Department of Defense networks.

---

[4] According to Department of Defense communication to Congress regarding its purchase of online balloting systems from Everyone Counts and others, the systems were purchased to deliver blank ballots online, allow a voter to mark the ballot and then print the ballot for return by mail; the systems are not to be used to send the voted ballot back over the Internet. The communication reads "[t]he voter will be able to mark the ballot with all selected candidates,[...] and then print the ballot with State specific casting instructions and pre-addressed envelope for the voter to print out with a hard copy, sign with a wet signature and return by postal mail. These systems are the same as the front end of what a voter would experience in a full internet voting system. The [system] stops the online process at the online marking of the ballot and supports the postal return of a hard-copy, "wet" signature ballot."
http://comptroller.defense.gov/defbudget/fy2012/budget_justification/pdfs/03_RDT_and_E/DHRA.pdf

Even if used solely for military voters, the Internet voting systems available today do not utilize a secure, DoD network. These systems used today connect to the public Internet and are subject to attack from hackers anywhere in the world.

Misconception: Internet voting system vendors have developed ground-breaking systems that utilize military Common Access Cards or CACs and this will ensure system security. Members of the military are issued CAC cards which include a smartchip for logging onto secure military networks, but there are no online voting systems available today which use CACs to secure and encrypt ballots online. One vendor is claiming its system uses CACs to provide security but the use is limited to scanning or photographing the CAC and sending this data to the elections office to provide voter authentication. This is approximately the equivalent of requiring a voter to take a photo of his or her driver's license and sending it to the election's office to verify the voter's identification. This does improve the level of voter authentication, but this use of the CACs, which is what is being promoted currently, does nothing to secure the transmission of the voted ballot.

Misconception: Internet voting systems can be accurately audited. Vendors often claim that their systems can be audited but it is impossible to conduct a meaningful audit of ballots sent over the Internet. Because there are many different attack vectors which could alter a voter's ballot without his or her knowledge, and which would be imperceptible to the vendor or election official, and because we vote by secret ballot, it is virtually impossible to conduct a meaningful audit of an election in which ballots are transmitted over the Internet. Attacks which modify votes before they leave the voter's computer would be undetectable, just as attacks on banking systems that transfer funds without the account owner's permission are undetectable[5]. According to the National Institute of Standards and Technology or NIST, "ensuring remote electronic voting systems are auditable largely remains a challenging problem, with no current or proposed technologies offering a viable solution."[6]

Thank you again for the opportunity to testify today. I am happy to answer any questions.

[5] However, in the case of funds stolen through malicious software in the user's computer, the lost funds may be recoverable because of Federal laws limiting retail banking losses. These limits do not apply to commercial bank accounts.

[6] http://www.nist.gov/itl/vote/uocava.cfm

New York
COMMON CAUSE
Holding Power Accountable

TESTIMONY OF SUSAN LERNER
EXECUTIVE DIRECTOR, COMMON CAUSE/NY
BEFORE THE NEW YORK CITY COUNCIL COMMITTEES ON
GOVERNMENTAL OPERATIONS AND TECHNOLOGY
December 18, 2013

Thank you for the opportunity to address you today. I am Susan Lerner, Executive Director of Common Cause/New York. Common Cause is a national nonpartisan, nonprofit public advocacy organization founded in New York in 1970 by John Gardner as a vehicle for citizens to make their voices heard in the political process and to hold their elected leaders accountable to the public interest. With nearly 400,000 members and supporters and 36 state organizations, Common Cause is committed to honest, open and accountable government and to encourage citizen participation in democracy. Since its inception, the New York chapter has always been and continues to be one of the most active state chapters in the country, representing tens of thousands of New Yorkers throughout the state.

In accord with our overall mission we have consistently advocated for election reform, working to improve accessibility, accuracy, transparency, and verifiability in our democratic process at the city, state and national level. For a number of years, our research arm, Common Cause Education Fund, has conducted comprehensive studies of how we conduct elections, which studies look at voting issues across the country and also examine different reforms as actually implemented in various states as well as in other countries. Here in New York, Common Cause is a co-facilitator, along with NYPIRG, of the state coalition of groups that monitor election activities, now called the New York State Voters' Coalition. Common Cause NY has spent decades working to expand voting rights, to ensure that every New York State citizen that wants to vote has the opportunity to do so, and be certain that their vote is counted as cast.

We are committed to expanding and easing access to the voting booth and ballot box for all citizens but we must not rush to adopt policies and technology that are not secure and would risk the integrity and trustworthiness of our election system. There is growing interest in voting over the Internet, as this is seen as a way to facilitate ballot access, especially for military and overseas voters. But we cannot support online voting because the security risks are just too grave. While it is true that thirty states currently allow some form of email, fax or electronic ballot return that does not mean it is safe or secure. Most of those states passed bills to allow voted ballots to be returned over the Internet by email or electronic transmission *before* the severity of the risk of cyber attack was fully understood or recognized. In recent years national cyber security experts have sounded increasingly urgent warnings that the Internet is highly insecure, impossible to safeguard absolutely, rich with possible avenues of attack, and rife with potential attackers.

With alarming frequency, networks with the most robust security protocols are being penetrated by attackers. According to National Intelligence Director James Clapper, cyber attacks have surpassed terrorism as the top threat to U.S. national security.[1] Attackers have successfully

[1] Susskind, Jane, "*Cyber Security Not Terrorism, Number One Threat to National Security,*" IVS.US, Mar 15, 2013

penetrated the most hardened and secured networks including the CIA, FBI, Google, Sony and Department of Defense.[2] It is naïve to presume that a system designed for voting over the Internet can resist attacks more successfully than the nation's most fortified networks.

Allowing ballots to be cast by email, efax, or through Internet portals - at least with the current security tools - is an invitation to partisan operatives and nation states to tamper with the integrity of our elections. The problem is particularly pernicious because it is unlikely that such attacks will be discovered. Because we vote by secret ballot it would be difficult if not impossible to detect a cyber attack on an online election.

As the federal agency responsible for setting voting system standards and researching Internet voting, the **National Institute of Standards and Technology** (NIST) determined that too many of the security challenges inherent with Internet voting cannot be resolved or adequately mitigated with the computer security tools currently available. NIST concluded that secure Internet voting is not yet feasible and that more research is needed.[3] ***Any claim by a vendor that it has developed a secure Internet voting system is in direct contradiction to NIST's best assessment after years of research and analysis.***

Likewise, the **Federal Voting Assistance Program** (FVAP) at the **Department of Defense** does not advocate for online voting for the military because of the security risks. FVAP considers postal mail return the most responsible method of voting for military voters. In its report "2010 Electronic Voting Support Wizard Technology Pilot Program to Congress" released May 2013 FVAP stated:

"Due to unresolved security concerns regarding the electronic return of voted ballots, FVAP purposefully designed the EVSW project to refrain from considering that aspect and remain in alignment with previous efforts without injecting concerns over security over the use of the internet. Electronic delivery of a blank ballot, when combined with the postal return of the voted ballot, remains the most responsible method for moving forward until such time applicable Federal security guidelines are adopted by the EAC."

We must heed the cautions of our national and computer security experts and recognize that Internet voting is just too dangerous, and our democracy is too precious to risk putting our elections online.

---

[2] http://csis.org/publication/cyber-events-2006
[3] http://www.nist.gov/itl/vote/uocava.cfm

CNN – POLITICALTICKER –December 17, 2013
http://politicalticker.blogs.cnn.com/2013/12/17/report-chinese-hackers-attacked-crucial-government-election-website/

Washington (CNN) - Chinese hackers tapped into the Federal Election Commission's website during the federal government shutdown in October, a report released Tuesday by an investigative news organization says.

The report from the Center for Public Integrity, one of the country's oldest and largest nonpartisan, nonprofit investigative news organizations, indicates that hackers crashed the FEC's computer systems, which compiles federal election campaign finance information like contributions to parties and candidates, and how those billions of dollars are spent in each election by candidates, political parties, and independent groups such as political action committees.

The attack came as nearly all of the FEC's employees, except for the presidential-appointed commissioners, were furloughed due to the government shutdown, with not even one staffer being deemed "necessary to the prevention of imminent threats" to federal property. And it came a few months after an independent auditor hired by the government warned that the FEC's computer systems were at "high risk" to infiltration, a charge the commission disputed.

"Hackers from China, in Russia, Syria, you name it are constantly targeting U.S. websites. But what happened here with the Federal Election Commission, which is the independent watchdog sponsored by the government to keep elections fair and free, effectively got hit about as hard as it ever has gotten hit," David Levinthal of the Center for Public Integrity said on CNN's "New Day."

"It came as the FEC had absolutely no regular employees actually serving at the agency because of the government shutdown. It was one of the agencies that actually went completely dark during the government shutdown, only had the commissioners themselves manning the doors, manning the systems. They are not IT experts by any stretch of the imagination," Levinthal told CNN's Chris Cuomo.

The CPI says the hacking incident was confirmed by three government officials involved in an ongoing investigation that included the Department of Homeland Security.

"Here you have for days at a time, the FEC's website - which is part and parcel of the agency's mission to provide Americans with the ability to access information about their elections, access information about political campaigns and candidates - and nobody in America could do it during that time. So it was a huge black eye, not only for the agency but for the country's government in general," Levinthal added.

The FEC is not commenting at this time about the hacking incident.

Following the hacking incident, the FEC in November said it had moved certain data servers off-line and replace them with less powerful backup servers, that the agency said would slow the ability for users to navigate the website.

Testimony
Global Gateway Alliance Executive Director Stephen Sigmund
In Support of Resolution 1954

My name is Stephen Sigmund and I am the Executive Director of the Global Gateway Alliance. GGA is a business, labor, academia and government coalition whose mission is to advocate for modernization of NYC area airports and related infrastructure.

Our Board is made up of New York and New Jersey leaders like our founder Joe Sitt of Thor Equities, Association for a Better New York and the Teamsters which are represented today, the Partnership for New York City, Retail Wholesale and Department Store Union and the New York Hotel Trades Council, NYU Rudin Transportation Center, TD Bank and many others.

We are here today in full support of Resolution 1954.

Earlier this year, GGA conducted a survey showing 15 out of the 20 busiest US airports provide free Wi-Fi. That list includes major hubs, and major competitor cities, like Boston, Los Angeles, and San Francisco.

In fact, our airports comprise 3 of the 5 that don't have free Wi-Fi (Miami and Chicago)

The 2012 Travel and Leisure study which ranked New York area airports the worst in the country specifically cited our lack of free Wi-Fi and the difficulty in even finding a Wi-Fi signal at all after paying for it.

Just as important, free Wi-Fi has become an expected convenience, and quality of life improvement, throughout NYC Public Places. As of 2012, in NYC, free public Wi-Fi is available in 20 parks, 5 subway stations, public libraries and museums throughout the City, 20 public pay phones, and countless restaurants, coffee shops, and other locations.

As you can see on the chart behind me, there is free Wi-Fi essentially everywhere in our region – except our airports.

With our airports the most delayed in the country and so much extra time needed for security, passengers need their mobile lives to extend to the airports. In particular, business travelers rely on good mobile connections wherever they are on the road. A full 70% of passengers carry smart phones, and 90% of airline passengers would give up at least one other onboard convenience for a Wi-Fi connection.

GGA supports Council Member Brewer's resolution whole heartedly, and we urge its passage in the full Council. We join in calling on Boingo to amend its contract with the Port Authority, which is archaic by Internet standards, and allow passengers free Wi-Fi.

NYC airports should be leading the country, not so far behind every other airport and public space in the country.

Thank you.

TESTIMONY FROM THE ASSOCIATION FOR A BETTER NEW YORK REGARDING INTERNET ACCESS AT AIRPORTS BEFORE THE NYC COUNCIL JOINT COMMITTEES ON GOVERNMENT OPERATIONS AND TECHNOLOGY
December 18, 2013

Good Morning. My name is Jordan Isenstadt and I am the Deputy Director of the Association for a Better New York (ABNY). ABNY is one of New York's longstanding civic organizations advocating for the policies, programs and projects that make New York a better place to live, work and visit. We represent the broad fabric of New York's economy, and our membership includes New York's most influential businesses, non-profits, arts & culture organization, educational institutions, labor unions and entrepreneurs. We remain firmly dedicated to the constant growth and renewal of New York City's people, businesses and communities.

I am here this morning to offer ABNY's support of Resolution 1954, which calls upon the Port Authority of New York and New Jersey to amend its contract with Boingo Wireless, in order to provide free Internet access at its three major airports. Thank you Councilmember Brewer for introducing this resolution that is vital for business travelers and the City as a whole.

For millions of business travelers, airports are an extension of their office. In fact, 55% of all business travelers carry three to four smart devices at all times. Access to free and reliable Wi-Fi at airports is just another part of keeping business running smoothly and efficiently, especially given the increase in time spent at the airport due to long lines at security checkpoints and frequent delays.

A vast majority of global airports say they now offer travelers free Wi-Fi, but the New York City airports, with its 110 million passengers, and JFK having the most international arrivals, are still without free Wi-Fi, which seems incomprehensible. Airports account for $63B in regional economic activity and nearly half a million jobs in the New York City area alone. It simply makes no sense that our airports do not have the expected convenience of public Wi-Fi.

This is not a situation where we need to "reinvent the wheel", as countless airports around the world have instituted free Wi-Fi offerings and now the Port Authority needs to do the same. This resolution will make a difference to thousands of travelers each day. We thank the New York City Council Subcommittee on Government Operations and Technology for considering this important issue.

Thank you for the opportunity to testify.

###

Association for a Better New York
355 Lexington Avenue, 8th Floor, New York, NY 10017
T: (212) 370-5800 F: (212) 661-5877 E: info@abny.org

JOINT COUNCIL No.16

INTERNATIONAL BROTHERHOOD OF TEAMSTERS

265 WEST 14TH STRET– SUITE 1201
NEW YORK, NEW YORK 10011
(212) 924-0002
FAX (212) 691-7074

NYC Council: Committee on Technology
December 18. 2013

Resolution 1954 to provide free WiFi at NYC airports

Hello, my name is Rebecca Lynch and I am here on behalf of Teamsters Joint Council 16 representing 120,000 working men and women in the Greater New York area. Thank you for giving me the opportunity to speak before your committee on this resolution that will be beneficial to New Yorkers and the millions of visitors New York City receives annually.

As a board member of the Global Gateway Alliance, the Teamsters recognize the importance of world-class airports. As a union that represents pilots, mechanics, cleaners and truckers in the nation's airports, we recognize the importance of world-class airports for the great number of jobs they create.

The Global Gateway Alliance study with the Partnership for New York City found that almost half a million jobs are created by our airports. Better amenities and options, such as the proposed wireless internet access, at our airports will lead to more amiable travel for New York's airport patrons and that in turn translates to increased business which leads to increased hiring from our communities and increased revenue for New York City, the air carriers, and the merchants in our airports.

A 2012 airport survey conducted by Travel and Leisure ranked LaGuardia Airport the worst airport in the United States, JFK and Newark Airports didn't fare much better. This is not the reputation we want and it is not what New York City should have. Something as simple as the proposed free Boingo wifi would make a world of difference for travelers in our New York City airports. Boingo has set a precedent, they have been offering a free, advertiser-supported wifi options since 2007. Since its

implementation, the usage has doubled. Wireless internet has a huge impact at airports- in Boston, over 20% of passengers take advantage of free wifi and in San Francisco, over 30%.

These numbers are not small and are constantly growing and our passengers deserve the same level of amenities they have come to expect in parks, subways, coffee shops, and airports around the world.

On behalf of the Teamsters Joint Council 16 and the residents and travelers of New York City, I want to thank you for this resolution and urge Boingo to amend its contract so we can begin planning the future of New York City's airports.

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: BRIAN KAVANAGH

Address: 237 FIRST AVE STE 407

I represent: NYS ASSEMBLY, 74TH DIST 10003

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: Dawn Sandow

Address: NYC Deputy Exec

I represent: NY BOE

Address: _____

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: Michael Ryan

Address: NYC Executive Director

I represent: NYC BOE

Address: _____

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☒ in opposition

Date: _____

(PLEASE PRINT)

Name: Susan Lerner

Address: 74 Trinity Pl, NY

I represent: Common Cause/NY

Address: 74 Trinity

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☒ in opposition

Date: 12/18/13

(PLEASE PRINT)

Name: Kate Doran

Address: 11 Polhemus Pl, Bklyn, NY 11215

I represent: League of Women Voters NYC

Address: 4 West 43rd St, NY, NY 10036

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: Eric Friedman

Address: _____

I represent: NYC Campaign Finance Board

Address: 40 Rector St NY NY 10006

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. _____

☐ in favor ☐ in opposition

Date: _____

(PLEASE PRINT)

Name: Douglas Kellner

Address: _____

I represent: New York State Board of Elections

Address: 40 N. Pearl St Albany NY 12207

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 1954 Res. No. _____

☑ in favor ☐ in opposition

Date: 12/18/2013

(PLEASE PRINT)

Name: Rebecca Lynch

Address: 275 Seventh Avenue, Fl. 18

I represent: Teamsters Joint Council 16

Address: 265 W 14th Street, Suite 1201

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. _____ Res. No. 1954

☑ in favor ☐ in opposition

Date: 12/18/13

(PLEASE PRINT)

Name: Jordan Isenstadt

Address: 355 Lexington Ave, NY NY

I represent: ABNY

Address: _____

Please complete this card and return to the Sergeant-at-Arms

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. ________ Res. No. 1954

☒ in favor ☐ in opposition

Date: 12/18/15

(PLEASE PRINT)

Name: Stephen Sigmund

Address:

I represent: Global Gateway Alliance

Address:

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. ________ Res. No. ________

☐ in favor ☒ in opposition

Date:

(PLEASE PRINT)

Name: Susan Greenhalgh

Address: 10 Robbins Av

I represent: Verified Voting Foundation

Address: Carlsbad, CA

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. ________ Res. No. 1954

☐ in favor ☒ in opposition

Date:

(PLEASE PRINT)

Name: Catherine Skopic for Teresa Hommel

Address: 140 West Broadway, NY, NY, 10013

I represent: Teresa Hommel

Address: tahommel@earthlink.net

Please complete this card and return to the Sergeant-at-Arms