

# Experiences Implementing Usable MPC For Social Good

Mayank Varia

Hariri Institute, Boston University

*Based on joint work with*

- BU: Azer Bestavros, Eric Dunton, Frederick Jansen, Kyle Holzinger, Andrei Lapets, Nikolaj Volgushev
- UMass: Rose Kelly, Shannon Roberts
- MIT: Malte Schwarzkopf

with the help of many more...

# Caveats Upfront

## A talk on deployment of secure multi-party computation (MPC)

- Only semi-honest MPC is discussed (though recent results indicate malicious security is becoming feasible for such applications)
- The function being computed is quite simple, ergo...
- Performance of the MPC protocol itself is not a bottleneck

## An experience talk (not a theory talk)

- Little discussion of cryptography
- Focus on human and systems challenges
- A sample size of one application with three deployments, so other applications and deployments may give rise to different lessons

Social

~~Cryptographic~~ assumption: Pay equity is a desirable goal

# 100% Talent: The Boston Women's Compact (April 2013)

## WOMEN'S WORKFORCE COUNCIL

The Women's Workforce Council was established by Mayor Thomas M. Menino on April 9th, 2013— known nationwide as Equal Pay Day. The day marks how far into 2013 women need to work to earn what men earned in 2012. The first of its kind in the country, the Council's mission is to help transform Boston into the best city in the country for working women.

Members of the Council represent the financial, engineering, medical, law, technology and retail sectors, and include small business owners, entrepreneurs, senior executives, as well as academic, labor and nonprofit leaders.

The Council's first priority was to identify new and creative ways to help close the wage gap between working men and women, helping Boston become the first major city to achieve pay equity. This report outlines the Council's recommendations to employers throughout the city.



# The Initial Plan (December 2013)

## 100% TALENT

### *The Boston Women's Compact*

To make Greater Boston the premier place for working women in America, by closing the wage gap and removing the visible and invisible barriers to women's advancement. By doing so, we will build a more equitable workforce where all talent is cultivated and valued.



## GOAL 3

### *Evaluating Success*

Employers agree to participate in a biennial review to discuss successes and challenges, as well as contribute data to a report **compiled by a third-party** on the Compact's success to date. Employer-level data would not be identified in the report. The specific data to be reported will build on data already required by federal and state authorities and should not create an additional reporting burden.

# Toward Cryptographically Secure Data Analysis (July 2014)

## Initiative on Cities

FOR IMMEDIATE RELEASE: September 23, 2014

CONTACT: Kira Jastive, [617-358-1240](tel:617-358-1240) or [kjastive@bu.edu](mailto:kjastive@bu.edu)

(Boston) – Boston University’s Rafik B. Hariri Institute for Computing and Computational Science & Engineering today announced it has received funding from the National Science Foundation (NSF) to develop a “smart-city” cloud platform designed to streamline and strengthen multiple municipal functions. Called *SCOPE: A Smart-city Cloud-based Open Platform & Eco-system*, the project is designed to improve transportation, energy, public safety, asset management, and social services in the City of Boston and across Massachusetts.



## Multi-institution cloud security effort



National Science Foundation  
WHERE DISCOVERIES BEGIN

Press Release 14-089

### Expanding the breadth and impact of cybersecurity and privacy research

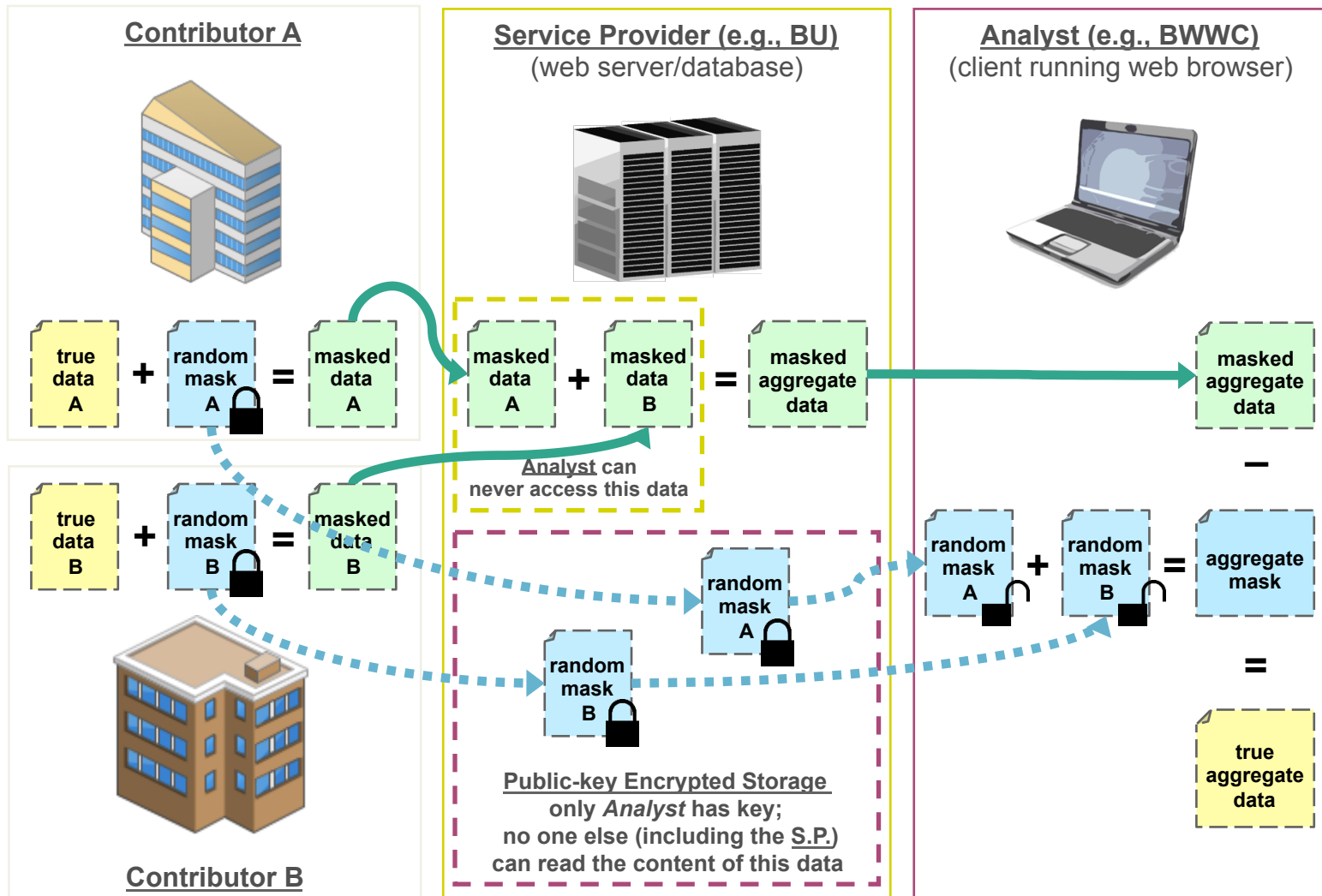
NSF announces two Frontier-scale projects, part of a \$74.5 million investment to support foundational cybersecurity research and education



Katharine Lusk

Lesson: To deploy MPC, find someone who has overpromised and cannot deliver

# Explaining MPC to Execs, HR, and Lawyers (2014-2015)



Lesson: Contextualize MPC's trust requirements

# Explaining MPC to Execs, HR, and Lawyers (2014-2015)

Lesson: Identify key participants whom you must convince





# Developing a Data Aggregation System (Spring 2015)

<https://100talent.org>

**Workforce Survey**  
Boston Women's Workforce Council

Enter Session Key

Email Address to track participation

**Female Workforce**

	Hispanic	White	Black	PacificIslander	Asian	NativeAmerican	Other	SumAnnCompJob	SumAnnCashPerJob	SumLenBnsJob
Executive										
MidLevel										
Professionals										
Technicians										
SalesWorkers										
AdminSupportWorkers										

**Male Workforce**

	Hispanic	White	Black	PacificIslander	Asian	NativeAmerican	Other	SumAnnCompJob	SumAnnCashPerJob	SumLenBnsJob
Executive										
MidLevel										
Professionals										
Technicians										
SalesWorkers										
AdminSupportWorkers										

- HR employees love spreadsheets
- Data contributors only need a web browser
- Modeled off of existing EEO-1 form

Branch: master ▾ [data-aggregator](#) / [client](#) / [script](#) / [ssCreate.js](#)

**frederickjansen** Update to use native pki and forge instead of jsencrypt

4 contributors

Executable File | 322 lines (288 sloc) | 11.6 KB

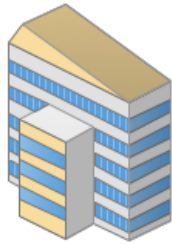
Lesson: Simplicity increases trust,  
which drives adoption

Lesson: Web browsers won the  
“corporate environment compatibility  
wars”

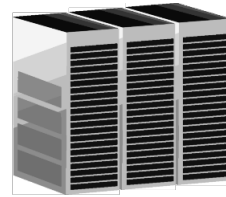
Lesson: Regulation -> standard schemas

# Developing a Data Aggregation System (Spring 2015)

## Contributors



## Service Provider (e.g., BU) (web server/database)



## Analyst (e.g., BWWC) (client running web browser)



## **Code Distributor**

## **Compute Service Provider**



### Boston University

- Extensive IT/engineering/CS expertise
- Production cloud environment

- Do not store data from individual contributors (liability)
- Do not store overall outcome (unnecessary)

- Incentive not to collude

## **Data Analyst**



### Boston Women's Workforce Council

- No IT staff or expertise
- Literate in statistical analysis

- Do not store data from individual contributors (liability)
- Store overall outcome (necessary for analysis)

- Incentive not to collude

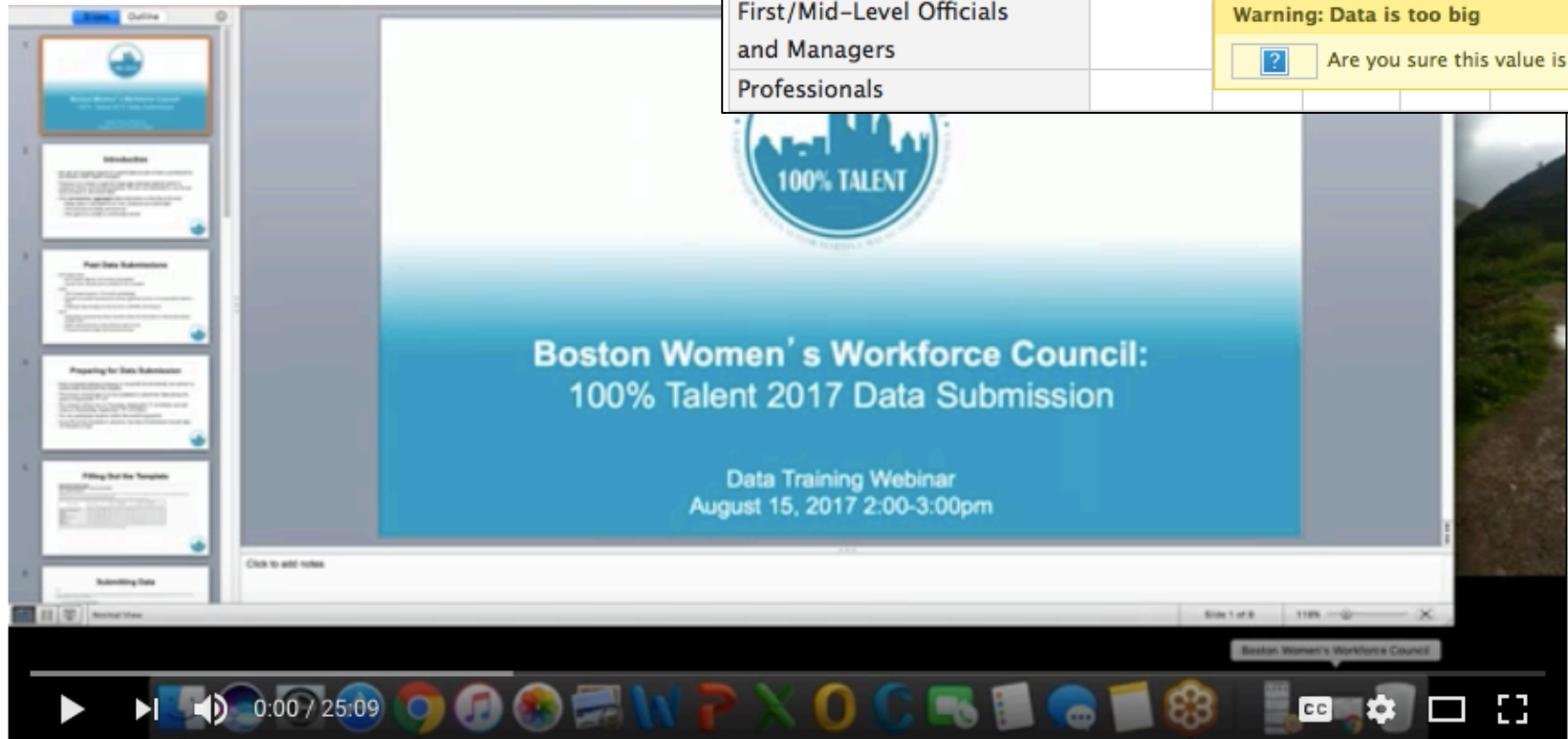
Lesson: Exploit asymmetry

# Explaining the Interface to Users (Spring 2015)

- Training sessions & videos
- Dry run with synthetic data
- Client-side error messages

Number Of Employees						
	Hispanic or Latinx		White		Black/African American	
	Female	Male	Female	Male	Female	Male
Executive/Senior Level Officials and Managers	100000					
First/Mid-Level Officials and Managers						
Professionals						

**Warning: Data is too big**  
 ? Are you sure this value is correct?



# June 8, 2015: D(ata Collection) Day

## Workforce Survey

Boston Women's Workforce Council



**Enter Session Key**

**Email Address to track participation**

**Female Workforce**

	Hispanic	White	Black	PacificIslander	Asian	NativeAmerican	Other	SumAnnCompJob	SumAnnCashtPerJob	SumLenSrcJob
Executive #										
MidLevel #										
Professionals #										
Technicians #										
SalesWorkers #										
AdminSupportWorkers #										

**Male Workforce**

	Hispanic	White	Black	PacificIslander	Asian	NativeAmerican	Other	SumAnnCompJob	SumAnnCashtPerJob	SumLenSrcJob
Executive #										
MidLevel #										
Professionals #										
Technicians #										
SalesWorkers #										
AdminSupportWorkers #										

Submit

June 6, 2015



**BOSTON WOMEN'S WAGE COMPACT  
DATA CONTRIBUTION AGREEMENT**

This Data Contribution Agreement (the "Agreement"), effective as of June \_\_, 2015 (the "Effective Date"), is entered into by and among the Simmons College ("Simmons"), Boston University, through its Rafik B. Hariri Institute for Computing and Computational Science and Engineering ("BU") and \_\_\_\_\_

In consideration of the mutual covenants, terms and conditions set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

**1. Scope.**

(a) The parties hereto wish to collaborate on a first-in-the-nation measurement that will capture the status of the gender wage gap within a set of companies. The parties desire to provide and collect data that will allow the wage gap to be measured in more precise ways. The results of the collaboration will be reflected in the resulting snapshot report ("Report") that will be completely anonymous with respect to the companies that provided data for the purposes thereof and will, in part, compare the status of the gender wage gap in the collaboration participants to that of all Boston employees, as written in the Boston Women's Workforce Council's 2013 Report, Boston: Closing the Wage Gap.

(b) Each party undertakes to each other party to use reasonable endeavors to perform and fulfill, promptly and actively, all of its obligations under this Agreement. Each party will contribute to the efficient flow of information and access to relevant data to ensure the effectiveness and efficiency of this collaboration. Each party undertakes to use reasonable endeavors to (i) notify the other parties promptly of any significant delay in performance; and (ii) inform the other parties of relevant communications it receives from third parties in relation to this collaboration or this Agreement. Each party shall use reasonable endeavors to ensure the accuracy of information or materials it supplies hereunder and promptly to correct any error therein of which it is notified. Each party shall be fully responsible for the supervision of its employees, agents and contractors and shall enter into appropriate arrangements for such purpose with its contractors. Each party will assign employees and/or other personnel of their respective organizations to carry out the work of the collaboration. Each employee and personnel assigned to work on the collaboration will continue to function in its role at the organization making the assignment. Each party will provide effective supervision for its employees and other personnel that they assign to collaborative activities and will retain responsibility and liability for the actions of such employees and other personnel. As among the parties to this Agreement, each party will be responsible for all costs and expenses incurred by such party in connection with this collaboration.

(c) The parties acknowledge and agree that the purpose and scope of this collaboration may be further refined and adjusted or changed throughout the Term (as defined below) by written agreement signed by each party. Any refinements, adjustments and changes shall be discussed in good faith amongst the parties and mutually agreed upon in writing prior to any party proceeding in a manner that reflects such refinements, adjustments or changes.

**2. Data Contribution.** \_\_\_\_\_ will deliver to Simmons and BU certain aggregate data, as agreed upon amongst the parties, for use in connection with this collaboration and the resulting Report (the "Data"). The Data shall be provided in a secure and confidential format, and the parties shall take appropriate steps to ensure the security and confidentiality of the Data.

thereof. Each of Simmons and BU shall have established prior to receipt of any of the Data, and shall continue to maintain for so long as Data is in its possession or control, generally accepted industry "best practices" systems security measures designed to guard against the destruction, loss, or alteration, of the Data that are no less rigorous than those maintained by it for its own information. Simmons and BU shall each maintain adequate administrative, technological and procedural access controls and system security requirements and devices necessary to protect the Data from: (a) threats or hazards to the privacy, confidentiality or integrity of the Data, (b) unauthorized or unauthenticated access to the Data; and (c) unlawful processing or accidental loss of, or destruction of or damage to, the Data.

**3. Rights in the Data and Resultant Data.**

(a) Simmons and BU each shall have the right to process and use the Data solely for purposes of the collaboration identified herein and in connection with the publication of the Report. Each of Simmons and BU hereby agree not to release specific information identified as a contributor of the Data or which identifies the source of the Data or any portion thereof. Simmons and BU will each bear the expense of incorporating the Data into the Report.

(b) The parties acknowledge and agree that \_\_\_\_\_ shall retain all rights to, owns and/or controls the Data and any other data, information and/or materials that are or may be useful for purposes of the collaboration conducted hereto. In addition, the parties acknowledge and agree that the Report shall not be published or otherwise disclosed prior to State Street's approval of the final version of the Report.

(c) Simmons and BU each have, reserve and retain all right, title and interest in and to all data, information, materials and other content of any type and in any format, medium or form that is processed by, for or on behalf of it by or through any device, system or network, including, but not limited to, any and all works, inventions, data, analyses and other information and materials resulting from the activities contemplated by this Agreement and all output, copies, reproductions, improvements, modifications, adaptations, translations and other derivative works thereof, based thereon or derived therefrom, other than the Data contributed hereunder (collectively, the "Resultant Data").

(d) Nothing contained in this Agreement will be construed as granting, by implication, waiver, estoppel or otherwise to Simmons and/or BU any right, title, or interest in or to the Data, except for the limited rights expressly granted to each Simmons and BU pursuant to this Agreement.

**4. Confidentiality.**

(a) "Confidential Information" means information that the Disclosing Party (as defined below) treats as confidential or

that confidential treatment will be afforded the Confidential Information.

**5. Warranties.**

(a) Each party represents and warrants to each other party that: (i) it has the full right, power and authority to enter into this Agreement and to perform its obligations hereunder; (ii) when executed and delivered by the party, this Agreement shall constitute the legal, valid and binding obligation of that party, enforceable against that party in accordance with its terms; and (iii) it is under no obligation to any third party that would interfere with its obligations under this Agreement.

(b) \_\_\_\_\_ has the unconditional and irrevocable right, power and authority to grant the rights hereunder to the Data pursuant to the terms of this Agreement; and

(c) EXCEPT AS EXPRESSLY SET FORTH ABOVE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EACH PARTY HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THIS AGREEMENT OR ANY SUBJECT MATTER HEREOF, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF NON-INFRINGEMENT.

**6. Limitations of Liability.** TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL ANY PARTY BE LIABLE FOR ANY LOSS OF, DAMAGE TO, OR CORRUPTION OF DATA, LOST PROFITS, BUSINESS, CONTRACTS, REVENUE, PRODUCTION, GOODWILL OR ANTICIPATED SAVINGS, OR BUSINESS INTERRUPTION OR OTHER COMMERCIAL, ECONOMIC OR OTHER DAMAGES, LOSSES OR INJURY OF ANY KIND, INCLUDING, BUT NOT LIMITED TO, ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR ANY SUBJECT MATTER HEREOF, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH LOSSES, DAMAGES OR INJURIES AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH IN THIS AGREEMENT FAILS OF ITS ESSENTIAL PURPOSE. The exclusions of damages set forth herein does not apply to a party's gross negligence, willful misconduct or fraud.

**7. Term and Termination.**

(a) This Agreement commences as of the Effective Date and will continue in effect until terminated as provided herein (the "Term").

(b) Any party may terminate this Agreement:

(i) at any time, without cause, and without incurring any obligation, liability or penalty by reason of such termination, upon at least thirty (30) days' prior written notice to the other parties; or

(ii) upon written notice to the other parties in the event that another party hereto has committed a material breach of the terms of this Agreement and such party has not cured such breach within thirty (30) days after receiving written notice of such breach from a non-breaching party.

(c) upon the expiration of the Term or the termination of this Agreement in accordance with this Section 7, each party shall (i) immediately discontinue all use of Confidential Information of any other party obtained hereunder; and (ii) promptly return or cause

Any purported assignment, delegation or transfer in violation of this Section is void. This Agreement is binding upon and inures to the benefit of the parties hereto and their respective permitted successors and assigns.

(e) **Amendment; Waiver.** This Agreement may only be amended, modified or supplemented by an agreement in writing signed by each party hereto. No waiver by any party of any of the provisions hereof shall be effective unless explicitly set forth in writing and signed by the party so waiving.

(f) **Severability.** If any term or provision of this Agreement is invalid, illegal or unenforceable in any jurisdiction, such invalidity, illegality or unenforceability shall not affect any other term or provision of this Agreement.

(g) **Governing Law; Jurisdiction.** This Agreement shall be governed by and construed in accordance with the internal laws of the Commonwealth of Massachusetts, without giving effect to any choice or conflict of law provision or rule. Neither the United Nations Convention on the International Sale of Goods nor the Uniform Computer Information Transactions Act shall have any application to this Agreement. Any legal suit, action or proceeding arising out of or related to this Agreement shall be instituted exclusively in the federal courts of the United States or the courts of the Commonwealth of Massachusetts in each case located in the city of Boston, and each party irrevocably submits to the exclusive jurisdiction of such courts in any such suit, action or proceeding.

(h) **Equitable Remedies.** Each party to this Agreement acknowledges and agrees that (i) a breach or threatened breach by such party of any of its obligations under this Agreement may give rise to irreparable harm to the other party for which monetary damages would not be an adequate remedy, and (ii) in the event of a breach or a threatened breach by such party of any such obligations, the other party shall, in addition to any and all other rights and remedies that may be available to such party at law, at equity or otherwise in respect of such breach, be entitled to seek equitable relief, without any requirement to post a bond or other security or to prove actual damages or that monetary damages will not afford an adequate remedy.

(i) **Export Regulations.** Simmons and BU each acknowledge and agree that it shall not export, or re-export directly or indirectly, the Data, to any country or person in violation of the laws and regulations of any applicable jurisdiction. This restriction expressly includes, but is not limited to, the export regulations of the United States of America.

This Agreement effective as of the date first above written.

Boston University, through its Rafik B. Hariri Institute for Computing and Computational Science and Engineering




By: Deane Baldwin  
Name: \_\_\_\_\_  
Title: Deane M. Baldwin  
Assistant Vice President, Sponsored Programs

6/8/15

Lesson: The lawyers will come for you... even if you build a technology whose main benefit is to keep the lawyers away

# June 8, 2015: D(ata Collection) Day

**Workforce Survey**  
Boston Women's Workforce Council

Enter Session Key

Email Address to track participation


Female Workforce

	Black	PacificIslander	Asian	NativeAmerican	Other	SumAnnCompJob	SumAnnCastPerfJob	SumL
Executive	#							
MidLevel	#							
Professionals	#							
Technicians	#							
SalesWorkers	#							
AdminSupportWorkers	#							
FoodWorkers	#							

Male Workforce

	Black	PacificIslander	Asian	NativeAmerican	Other	SumAnnCompJob	SumAnnCastPerfJob	SumLenSrcJob
Executive	#							
MidLevel	#							
Professionals	#							
Technicians	#							
SalesWorkers	#							
AdminSupportWorkers	#							
FoodWorkers	#							

**“If this does not work out, I will just fax you the spreadsheet for you to enter...”**



Lesson: Bottleneck/weak point of security solutions = human users  
(this threat cannot be removed, but it can be mitigated)

# Usability and Heuristic Evaluations

## Our chosen properties

- Familiar interface
- Compatibility
- Error detection/feedback
- Asynchrony
- Idempotence

## Standard usability components

- Learnability
- Efficiency (user productivity)
- Memorability
- (Low) errors
- Satisfaction

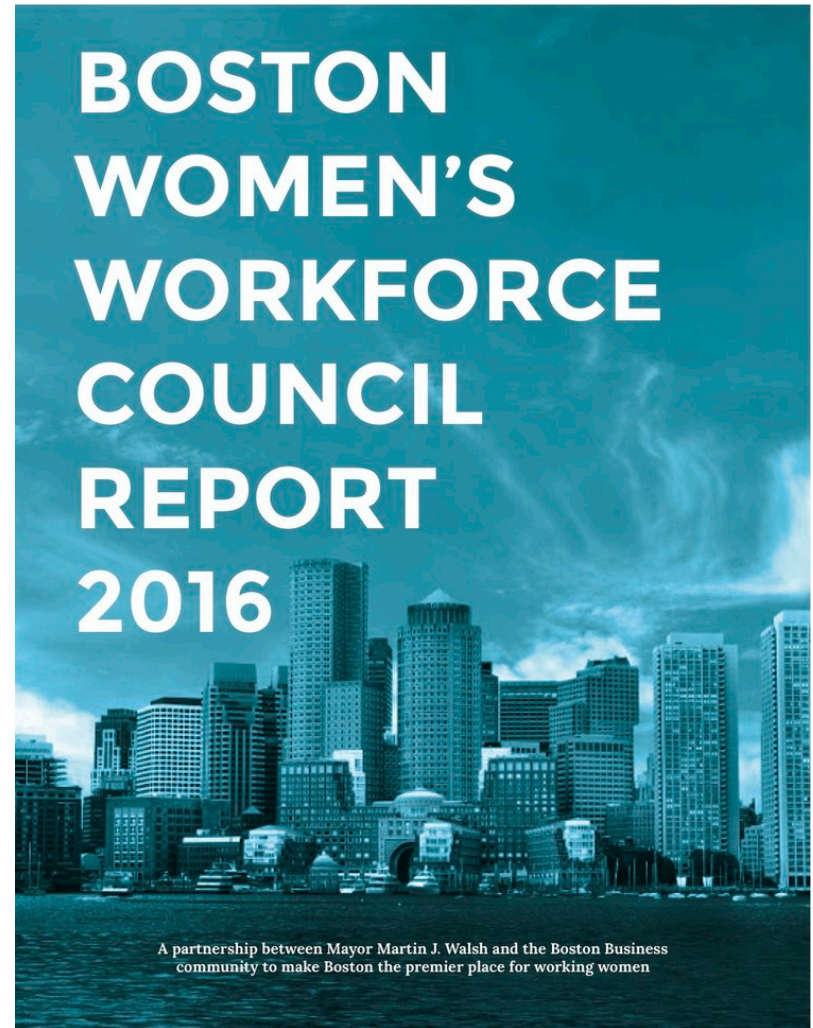
Lesson: When designing, implementing, and deploying any security tool, involve human factors experts from the start.

Heuristic Categorization and Number	Usability Issue	Average Rating
1.1	There is no indication as how much of the table has been or is yet to be completed.	4.5
1.2	There is no indication as to whether the session key is valid.	3.5
1.3	There is no indication as to whether the email address is valid.	1.5
1.4	After submission, user sees messages saying "loading" and then a confirmation window, which is confusing.	3
1.5	After submission, there is no information indicating that data can be resubmitted.	3.5
1.6	There is no email confirmation indicating that data was submitted.	2
2.1	The column and row headings do not use real-world terms that Human Resources (HR) uses, e.g., sum instead of total, workforce instead of employees, and mos. instead of months.	4.5
2.2	The tables are separated by gender, irrespective of whether HR data is usually separate by gender, e.g., if it is separated by ethnicity, it will be difficult for them to enter data separated by gender.	4.5
2.3	The table require a summation instead of an average, irrespective of whether HR data is given via averages or summations.	4
2.4	The columns requiring summary data (i.e., sum) are visually the same and not separated from data on raw numbers or monetary values.	2
2.5	The sum cells require one to calculate totals by hand.	3.5
2.6	When you drag to select the same value for multiple cells, the cells are highlighted in red, implying an error.	3.5
3.1	A cell is highlighted in red if a user clicks there, does not input a number, then clicks somewhere else.	5
3.2	Ctrl + Z (undo) is functional, but it always results in the previous cell being highlighted in red.	4
3.3	The meaning of the red cell is unclear.	5
3.4	Decimal points are not allowed in any cell.	4
4.1	The terms #, \$, and mos. are used in the row headings, but not the column headings.	3.5
4.2	The difference between multiple employee groups is unclear, e.g., executive versus mid-level.	5
4.3	There is no option for "other" employee, i.e., if they don't fall into one of the employee groups.	5
4.4	While there is an option for 2+ races, not including Hispanic/Latino, there is not an option for 2+ races, including Hispanic/Latino.	5
4.5	Some employee types end with the word worker, but others do not.	2.5
6.1	There is no objective or set of instructions indicating what and where information is to be entered as well as where users can find the session key or appropriate email address.	5
6.2	There are no definitions of the terms, e.g., executive, mid-level, and annual compensation	5
7.1	Though copy and paste works, if an empty cell is copied, the pasted cell will be highlighted in red, indicating that the copy and paste procedure did not work.	4
7.2	There is no way to enter functions into the cells, e.g., C2 = A2 + B2.	2
7.3	You can only drag cells to copy values either horizontally or vertically, not both.	2.5
8.1	Contrast between column and row fillings and text may be inadequate, i.e., black text on grey background may not be visible for some users.	4
8.2	Red cells are inappropriate for those who are color blind, which is 8 percent of all males.	5
9.1	There are no messages associated with the red cells.	5
9.2	There are no messages associated with the grey cells.	3.5
9.3	There is not a list of errors near the submit button that would indicate what needs to be fixed before submission is possible.	4
10.1	There is no help page, documentation, or instructions.	5

# Larger Collection (2016)

- Over 150 signatories (71 appeared on collection day)
- Aggregate data analyzed and published by the BWWC
- Data encompasses about 112,600 employees
  - > 10% of the greater Boston area workforce
  - about \$11 billion in wages
- 2017 collection: 200+ signatories, of which 120+ contributed data

Lesson: People will build up trust in your system, even if it's designed so they don't need to trust you





# Reactions



## The Boston Globe

The congresswoman, who had signed onto a bill addressing income disparity between men and women, was impressed by the relevance he outlined. *“It’s linking it back for the members of Congress,”* Clark said. *“Nobody would think, oh, the Paycheck Fairness Act, how is that tied into NSF funding?”*



BWWC co-chair Evelyn Murphy on secure MPC: *“Here, we’re beginning to show how to use this sophisticated computer science research for public programs.”*

# Reactions

BOSTON.COM SHOP NEW CAR DEALS

The Boston Globe **Business** TEXT SIZE | MANAGE ACCOUNT | LOG OUT

Search

NEWS METRO ARTS **BUSINESS** SPORTS OPINION POLITICS LIFESTYLE MAGAZINE TODAY'S PAPER

MARKETS TECHNOLOGY BETABOSTON

## Mayor Walsh pushes to gather data on gender wage gap

✉️ [f](#) [t](#) [g+](#) [in](#) 35



YOOREE KIM LOSORDO

In Boston, white women make 83 cents for every dollar that men make, according to the city.

By [Katie Johnston](#) | GLOBE STAFF APRIL 07, 2015

Mayor Martin J. Walsh waded into the controversy surrounding the gender wage gap Tuesday, announcing that he was set to launch an unparalleled effort to collect salary data from businesses throughout Boston, and that he had boosted the salaries of two top women on his own staff.

### Top 10 Trending Articles

**Most Viewed** Most Commented Most Shared

Return to action a long time coming for Patriots' Dion Lewis



# Summary of Lessons Learned

## Deployment opportunities for secure solutions

- Could deploy MPC when people have overpromised but cannot deliver on (usually simple) computations
- Legal restrictions, liabilities, and natural incentives can be opportunity
  - ...to deploy “secure” techniques and technologies in unexpected ways
  - ...to *simplify* solution requirements
- Specialize (to the scenario at hand) not just the protocol(s) but the trust and computing setup
  - identify target user profiles and level of detail and confidence they require
  - separate roles, functionalities, and infrastructure (then assign as appropriate)

## Human factors will play a role regardless of technical details

- May still be necessary to follow familiar traditions (NDAs)
- Human users are (still) a weak point when it comes to security
- Conceptual simplicity, artifact usability/compatibility, and community acceptance can drive confidence/adoption

# Thanks!

[multiparty.org](http://multiparty.org)