# Cryptographically Secure Data Analysis for Social Good

**Mayank Varia**
Boston University
@mvaria

# Valuable

# Toxic

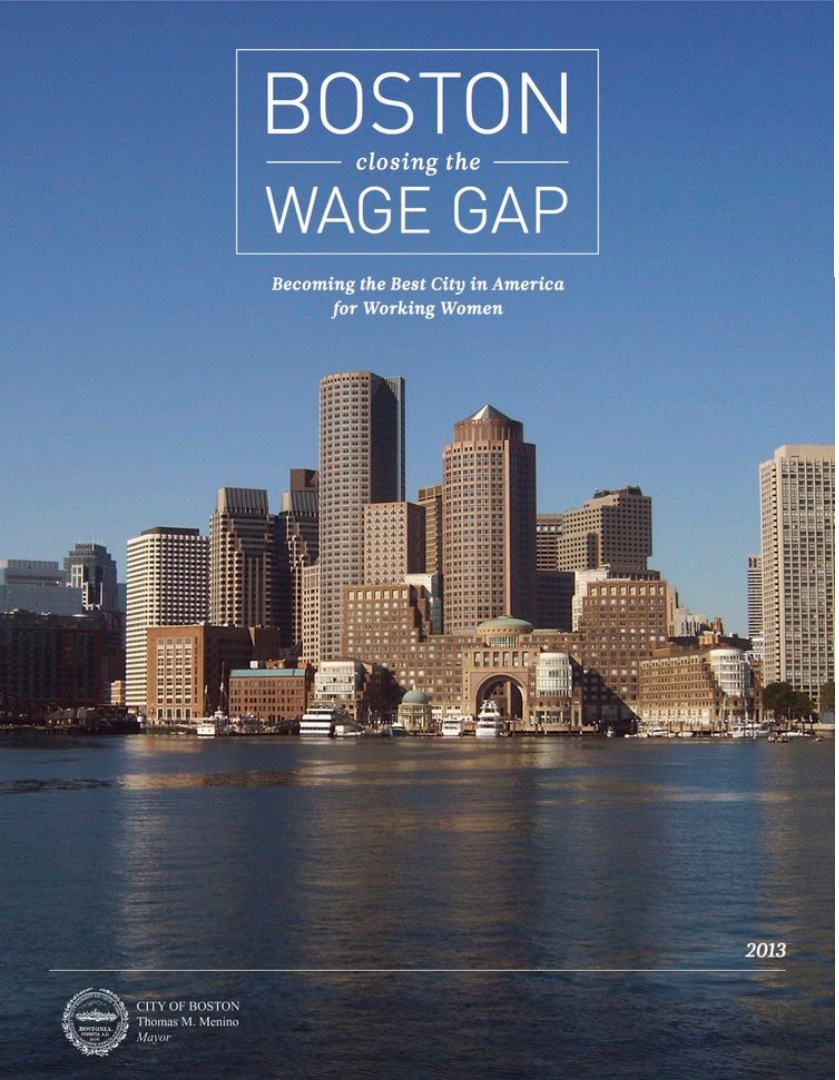

Images: Facebook, Wikipedia

# **Cryptography** *enables* **secure data analysis** *for* **social benefit**

Secure multi-party computation (MPC)

Employee salaries

Pay equity




# 100% TALENT

## The Boston Women's Compact

SIMMONS COLLEGE
BOSTON · MASSACHUSETTS

CITY OF BOSTON
Office of the Mayor
Martin J. Walsh

STATE STREET

EMC²
build smart

Raytheon

VERTEX

MassMutual
FINANCIAL GROUP

SUFFOLK

STAPLES
MAKE more HAPPEN

Putnam
INVESTMENTS

Care.com

aim
Associated Industries of Massachusetts

MASSACHUSETTS
TECHNOLOGY
COLLABORATIVE

Eastern Bank

FINAGLE A BAGEL

nationalgrid

EVERSOURCE
ENERGY

Abt
ASSOCIATES

BOLD
THINKERS
DRIVING
REAL-WORLD
IMPACT

BBK
WORLDWIDE

HILL HOLLIDAY

BJ's

MASSART
MASSACHUSETTS COLLEGE
OF ART AND DESIGN

WENTWORTH
Institute of Technology

PARTNERS
HEALTHCARE
FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL
AND MASSACHUSETTS GENERAL HOSPITAL

Charlestown
nursery school

Tech Networks of Boston
We're better together.

TUFTS Health Plan

WGA
WILLIAM
GALLAGHER
ASSOCIATES

WHEELOCK
COLLEGE

tBf The Boston Foundation
INNOVATION. INFORMATION. IMPACT.

Top it off

# Boston Women's Workforce Council

## 100% Talent Data Submission

### Number Of Employees

| | Hispanic or Latinx | | White | | Black/African American | | Native Hawaiian or Pacific Islander | | Asian | | American Indian/Alaska Native | | Two or More Races (Not Hispanic or Latinx) | | Unreported | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male |
| Executive/Senior Level Officials and Managers | | | | | | | | | | | | | | | | |
| First/Mid-Level Officials and Managers | | | | | | | | | | | | | | | | |
| Professionals | | | | | | | | | | | | | | | | |
| Technicians | | | | | | | | | | | | | | | | |
| Sales Workers | | | | | | | | | | | | | | | | |
| Administrative Support Workers | | | | | | | | | | | | | | | | |
| Craft Workers | | | | | | | | | | | | | | | | |
| Operatives | | | | | | | | | | | | | | | | |
| Laborers and Helpers | | | | | | | | | | | | | | | | |
| Service Workers | | | | | | | | | | | | | | | | |

# Boston Women's Workforce Council

## 100% Talent Data Submission

### Number Of Employees

| | Hispanic or Latinx | | White | | Black/African American | | Native Hawaiian or Pacific Islander | | Asian | | American Indian/Alaska Native | | Two or More Races (Not Hispanic or Latinx) | | Unreported | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male |
| Executive/Senior Level Officials and Managers | | | | | | | | | | | | | | | | |
| First/Mid-Level Officials and Managers | | | | | | | | | | | | | | | | |
| Professionals | | | | | | | | | | | | | | | | |
| Technicians | | | | | | | | | | | | | | | | |
| Sales Workers | | | | | | | | | | | | | | | | |
| Administrative Support Workers | | | | | | | | | | | | | | | | |
| Craft Workers | | | | | | | | | | | | | | | | |
| Operatives | | | | | | | | | | | | | | | | |
| Laborers and Helpers | | | | | | | | | | | | | | | | |
| Service Workers | | | | | | | | | | | | | | | | |

## Total Annual Compensation (Dollars)

| | Hispanic or Latinx | | White | | Black/African American | | Native Hawaiian or Pacific Islander | | Asian | | American Indian/Alaska Native | | Two or More Races (Not Hispanic or Latinx) | | Unreported | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male |
| Executive/Senior Level Officials and Managers | | | | | | | | | | | | | | | | |
| First/Mid-Level Officials and Managers | | | | | | | | | | | | | | | | |
| Professionals | | | | | | | | | | | | | | | | |
| Technicians | | | | | | | | | | | | | | | | |
| Sales Workers | | | | | | | | | | | | | | | | |
| Administrative Support Workers | | | | | | | | | | | | | | | | |
| Craft Workers | | | | | | | | | | | | | | | | |
| Operatives | | | | | | | | | | | | | | | | |
| Laborers and Helpers | | | | | | | | | | | | | | | | |
| Service Workers | | | | | | | | | | | | | | | | |

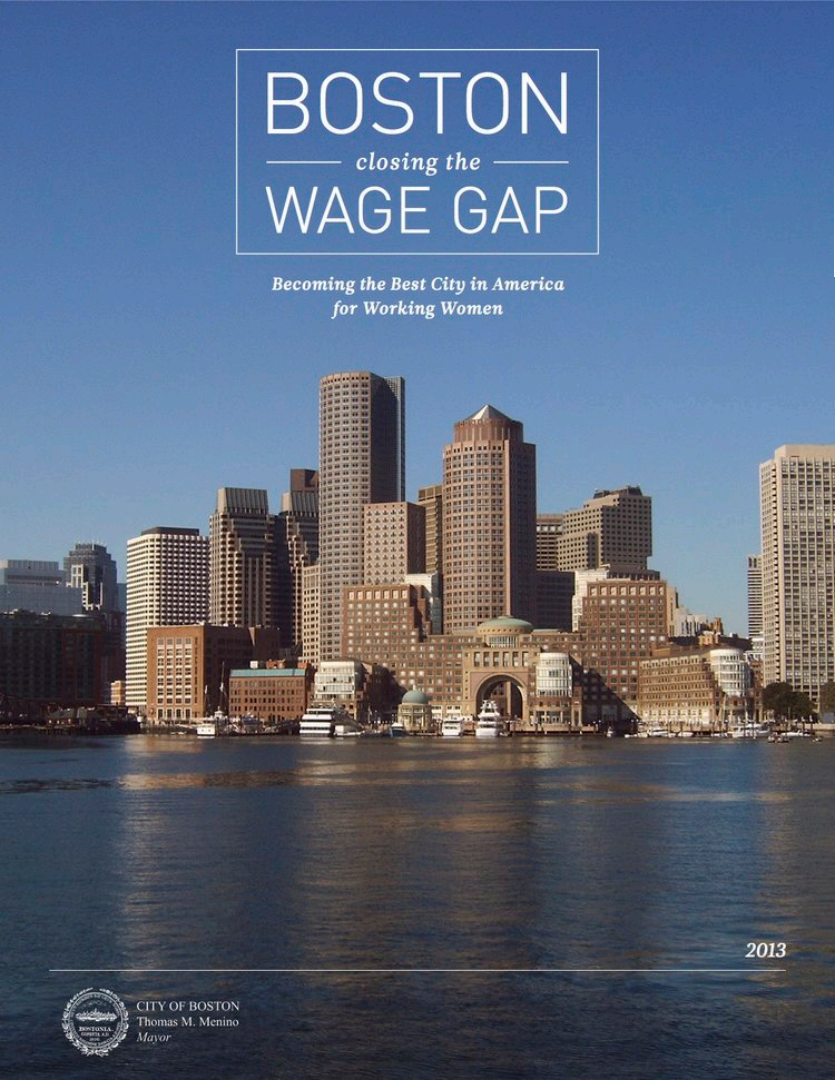
## Total Annual Cash Performance Pay (Dollars)

| | Hispanic or Latinx | | White | | Black/African American | | Native Hawaiian or Pacific Islander | | Asian | | American Indian/Alaska Native | | Two or More Races (Not Hispanic or Latinx) | | Unreported | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male |
| Executive/Senior Level Officials and Managers | | | | | | | | | | | | | | | | |
| First/Mid-Level Officials and Managers | | | | | | | | | | | | | | | | |
| Professionals | | | | | | | | | | | | | | | | |
| Technicians | | | | | | | | | | | | | | | | |

## Total Length of Service (Months)

| | Hispanic or Latinx | | White | | Black/African American | | Native Hawaiian or Pacific Islander | | Asian | | American Indian/Alaska Native | | Two or More Races (Not Hispanic or Latinx) | | Unreported | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male |
| Executive/Senior Level Officials and Managers | | | | | | | | | | | | | | | | |
| First/Mid-Level Officials and Managers | | | | | | | | | | | | | | | | |
| Professionals | | | | | | | | | | | | | | | | |
| Technicians | | | | | | | | | | | | | | | | |

Submit




# 100% TALENT

## The Boston Women's Compact

SIMMONS COLLEGE · STATE STREET · EMC²

### *Goal 3: Evaluating Success*

Employers agree to… 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.

TUFTS Health Plan · WGA WILLIAM GALLAGHER ASSOCIATES · WHEELOCK COLLEGE · tBf The Boston Foundation
INNOVATION. INFORMATION. IMPACT.
Top it off

# TRUST

# Trust Spectrum

**Trust us**

**Trust no one**

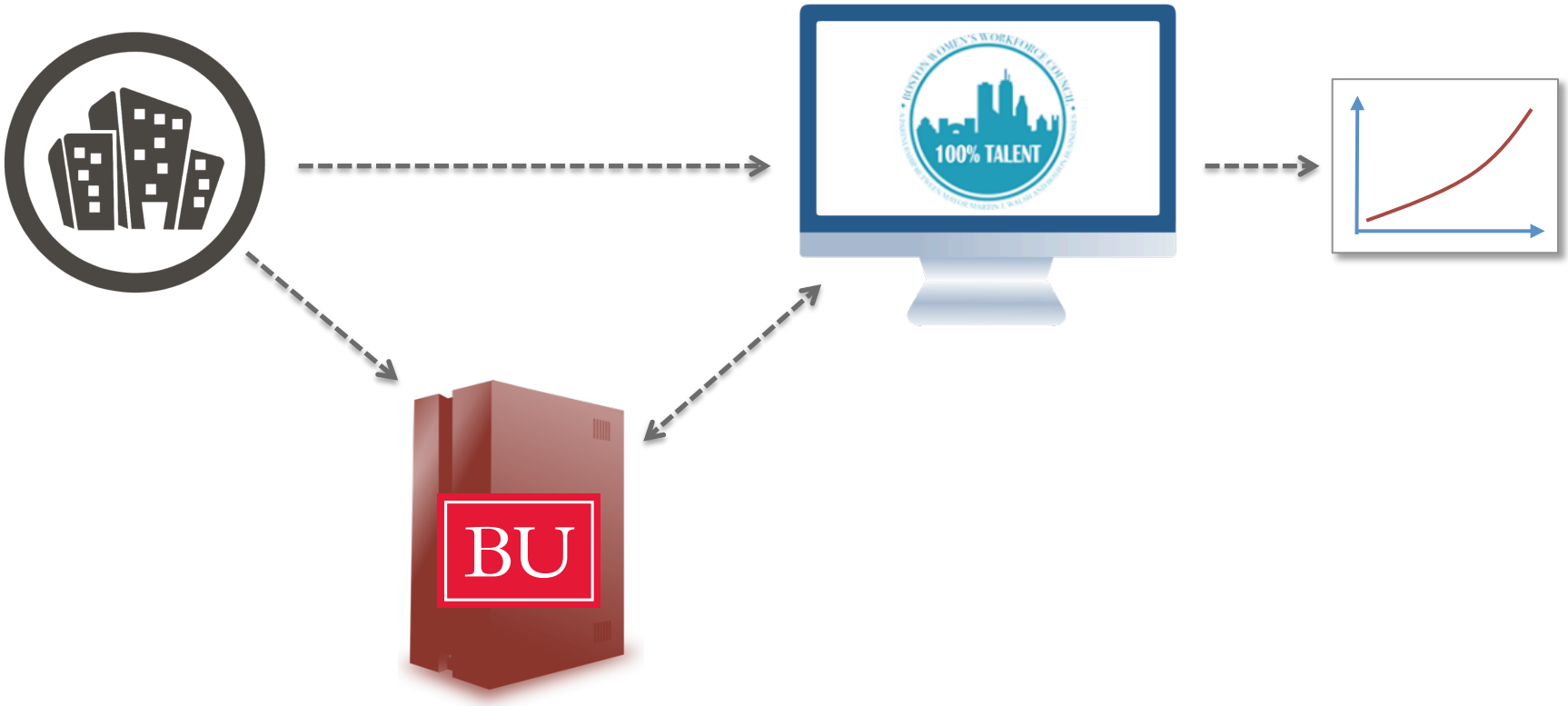
# Trust Spectrum

**Trust us** — **Trust anyone** — **Trust no one**

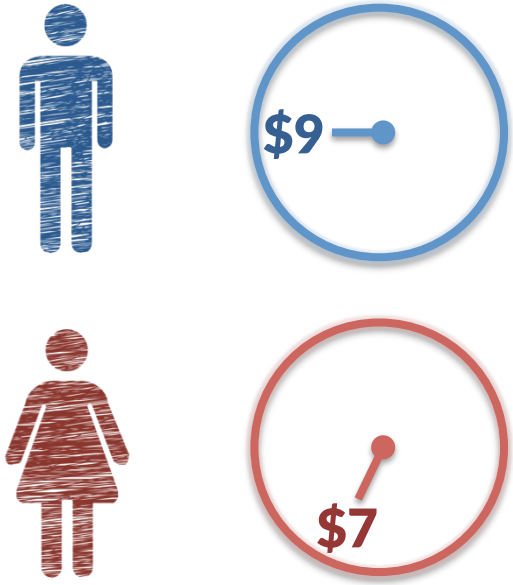
BU

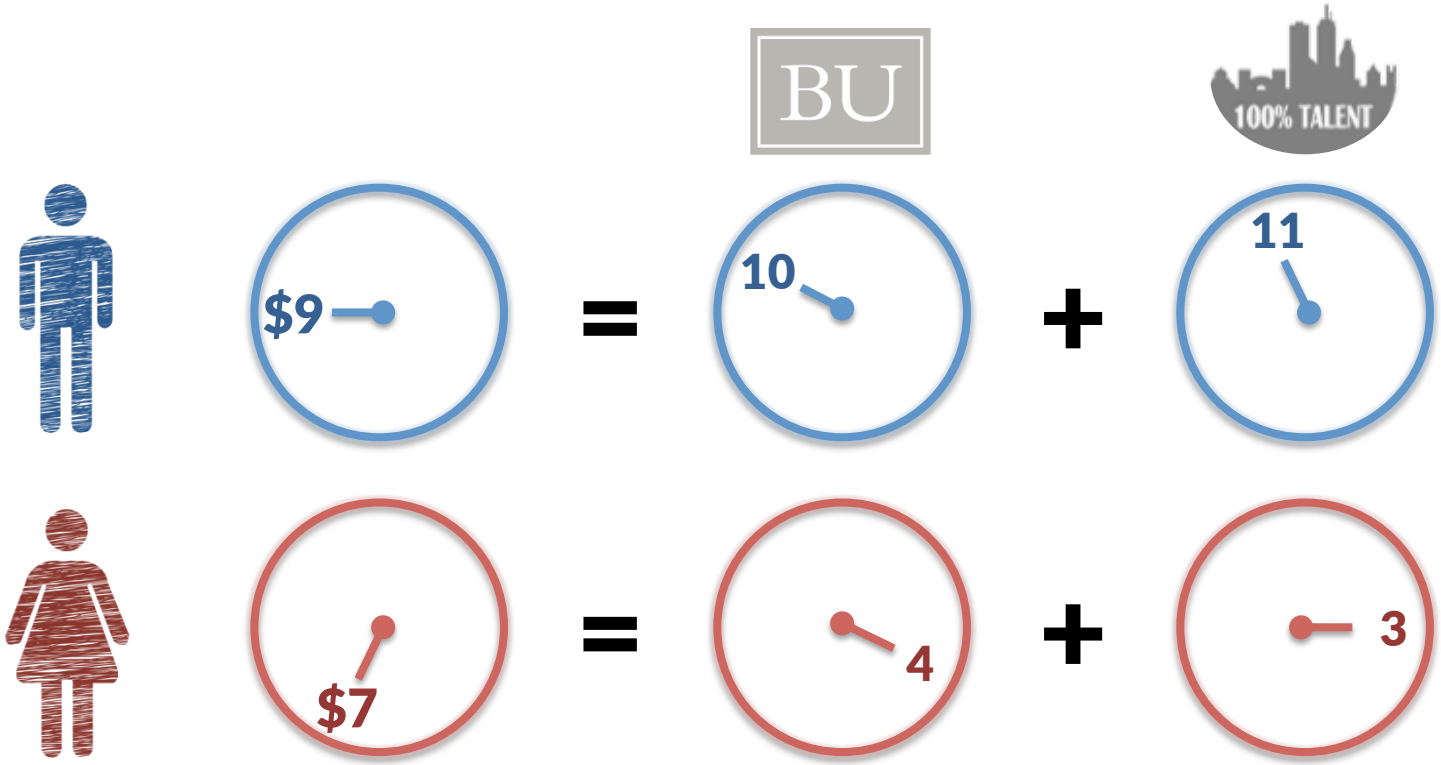
100% TALENT

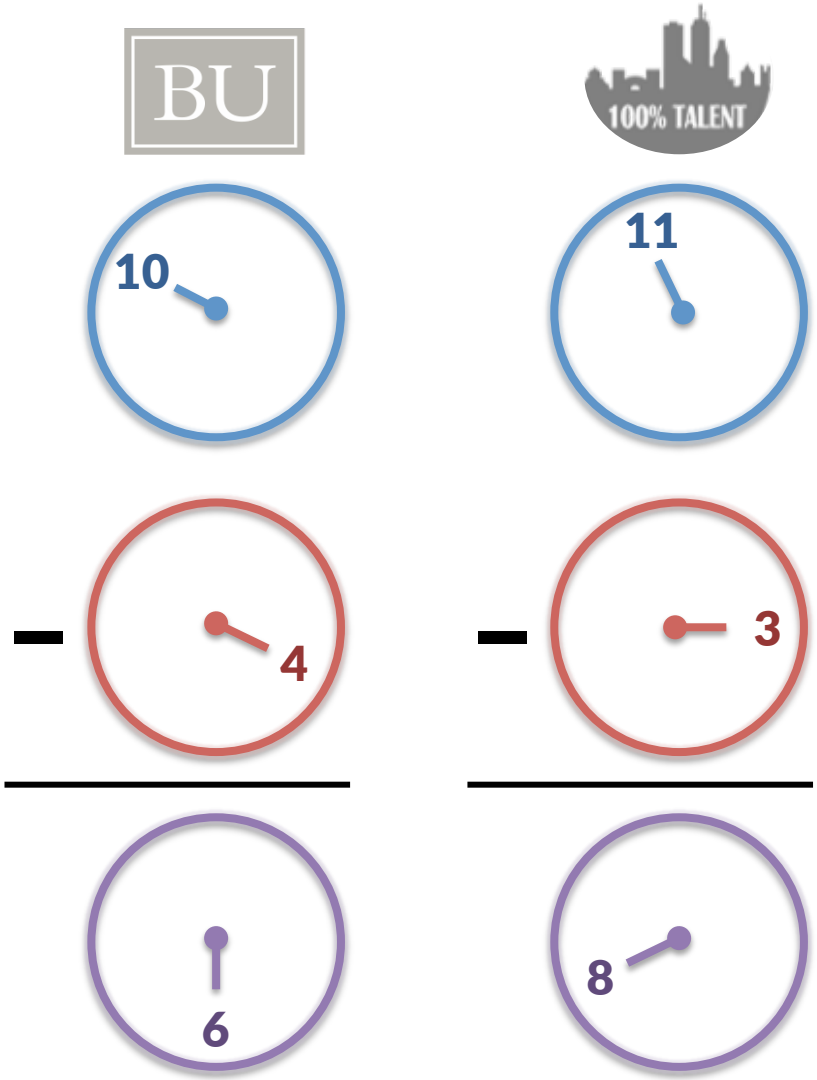
# Secure Multi-Party Computation (MPC)

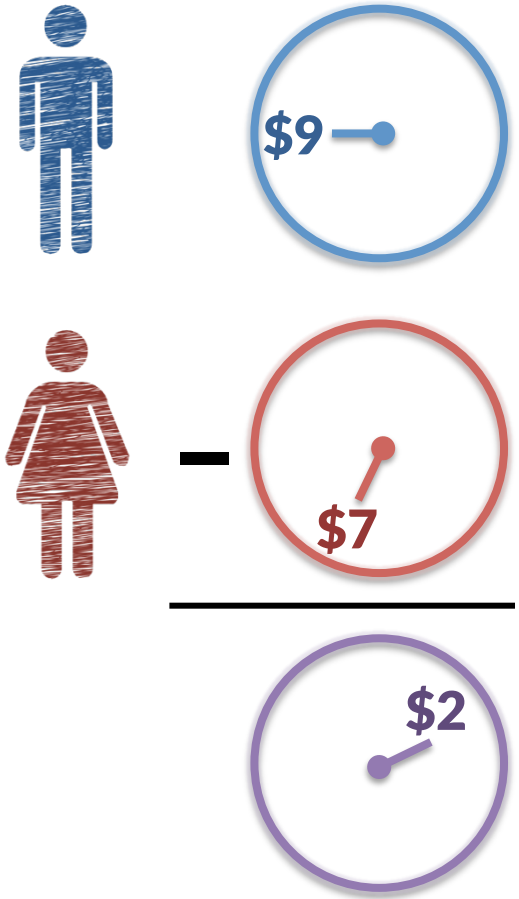


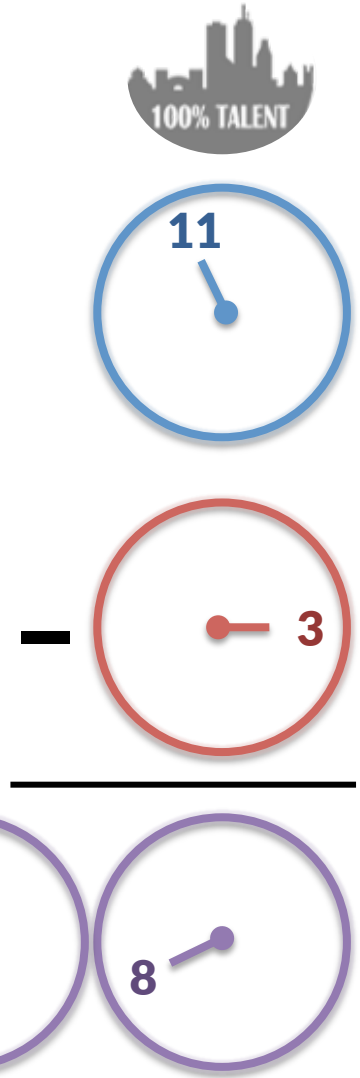
# HOW IT WORKS


$9
$7

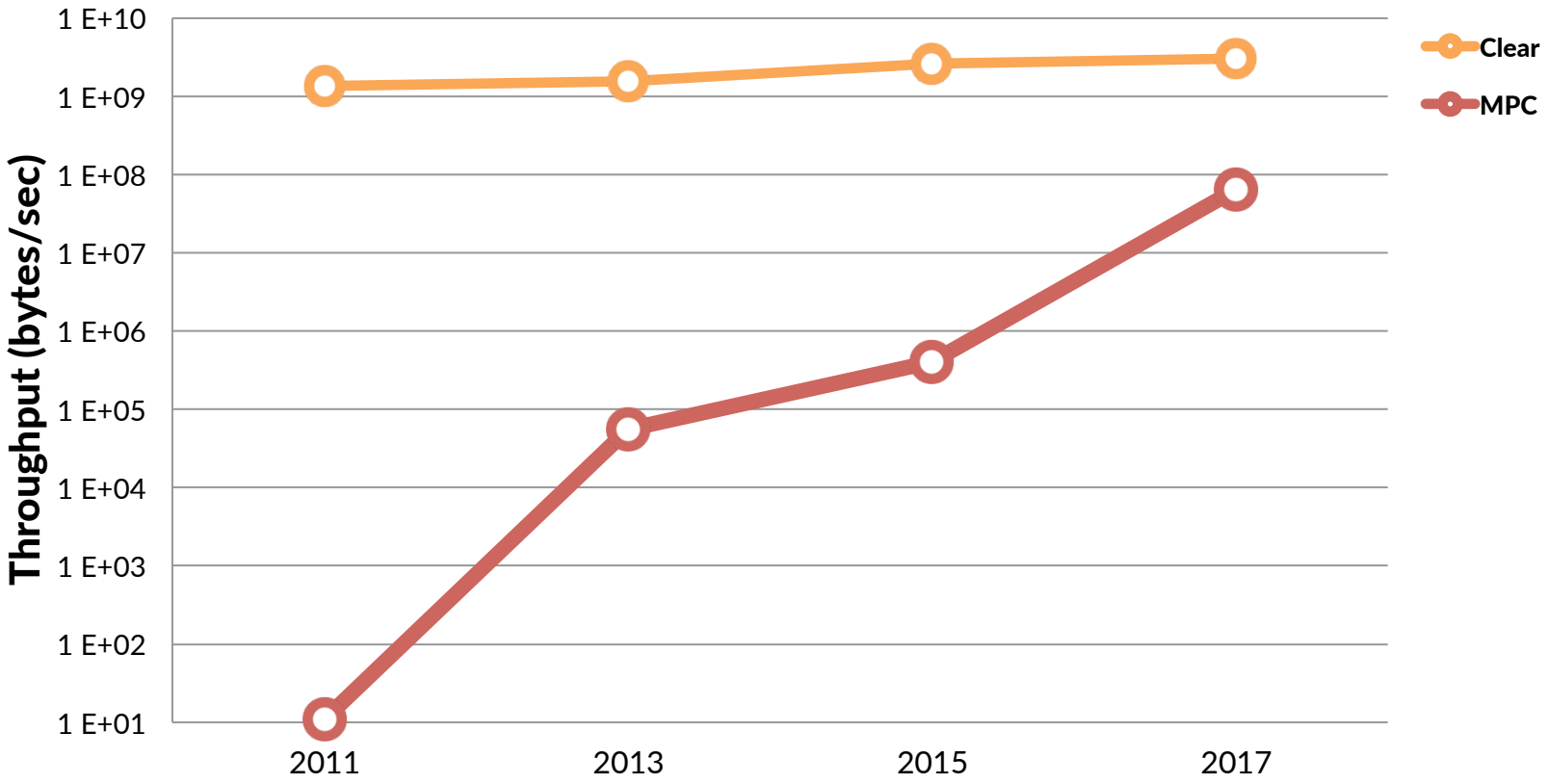

BU
100% TALENT
$9
=
10
+
11
$7
=
4
+
3


BU
100% TALENT
10
4
6
11
3
8


$9
$7
$2


100% TALENT
11
3
6
8

# Performance on AES




USABILITY

# Familiar

Number Of Employees

| | Hispanic or Latinx | | White | | Black/African American | | Native Hawaiian or Pacific Islander | | Asian | | American Indian/Alaska Native | | Two or More Races (Not Hispanic or Latinx) | | Unreported | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male | Female | Male |
| Executive/Senior Level Officials and Managers | | | | | | | | | | | | | | | | |
| First/Mid-Level Officials and Managers | | | | | | | | | | | | | | | | |
| Professionals | | | | | | | | | | | | | | | | |
| Technicians | | | | | | | | | | | | | | | | |
| Sales Workers | | | | | | | | | | | | | | | | |
| Administrative Support Workers | | | | | | | | | | | | | | | | |
| Craft Workers | | | | | | | | | | | | | | | | |
| Operatives | | | | | | | | | | | | | | | | |
| Laborers and Helpers | | | | | | | | | | | | | | | | |
| Service Workers | | | | | | | | | | | | | | | | |

# Reviewable

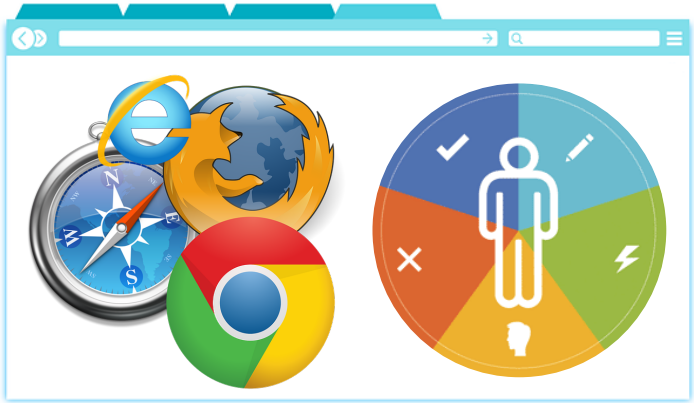
Number Of Employees

| | 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?

# Accessible



# Verifiable

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

github.com/multiparty

**Comprehension**

⇓

**Trust**

⇓

**Adoption**

**WomensWrkfrceCouncil**
@BostonWomenWork

Follow

#100PercentTalent Compact Signers learning about revolutionary MPC technology over lunch. How's that for a working lunch?

**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 [redacted]

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 any 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. [redacted] 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 delivered in an agreed-upon format and using an agreed-upon method that provides security and anonymity with respect to the Data and the provider 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 iden[redacted]it as a contributor of the Data or which identifies [redacted] 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 [redacted]old 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 proprietary, including, but not limited to, trade secrets, technology, information pertaining to business operations and strategies, and information pertaining to customers, pricing and 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.

([redacted] has the unconditional and irrevocable right, powe[redacted]y 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 obligations under Sections 3 or 4 or in the event of 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 to be returned to such other party or destroy or cause to be destroyed all copies obtained, made or authorized to be made hereunder of documents and tangible materials containing, reflecting, incorporating or based on any Confidential Information of such other party, and certify in writing to such other party that it

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.

ed 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: Diane Baldwin

Name:

Title: Diane M. Baldwin
**Assistant Vice President, Sponsored Programs**

6/8/15

## Employers

| | |
|---|---|
| 2016 | 69 |
| 2017 | 114 |

## Employees

| | |
|---|---|
| 2016 | 113k |
| 2017 | 167k |

Image: Wikipedia

**Mayor Martin J. Walsh:**
“This [is] the first time actual wage data has been reported both anonymously and voluntarily. This is a groundbreaking moment in tackling the gender gap.”

**Rep. Katherine Clark:**
“Nobody would think, oh, the Paycheck Fairness Act, how is that tied into NSF funding?”

115TH CONGRESS
1ST SESSION

**S. _____**

IN THE SENATE OF THE UNITED STATES

Mr. WYDEN (for himself, Mr. RUBIO, and Mr. WARNER) introduced the following bill; which was read twice and referred to the Committee on

"in designing, establishing, and maintaining the higher education data system, … the Commissioner shall use secure multiparty computation technologies"

115TH CONGRESS
1ST SESSION

**H. R. 4174**

IN THE SENATE OF THE UNITED STATES

NOVEMBER 16, 2017

Received; read twice and referred to the Committee on Homeland Security and Governmental Affairs

"establishment of a shared service to facilitate data sharing, enable data linkage, and develop privacy enhancing techniques"

# **Cryptography** *enables* **secure data analysis** *for* **social benefit**

multiparty.org

@mvaria