DEPLOYING MPC FOR SOCIAL GOOD

Lucy Qin

Research Software Engineer | Software & Application Innovation Lab | Boston University

Andrei Lapets, Frederick Jansen, Kinan Bab, Peter Flockhart,
Rawane Issa, Mayank Varia, Azer Bestavros

Software & Application
Innovation Lab

BOSTON
UNIVERSITY

MPC FOR SOCIAL GOOD

Hey,Charlie

Combatting Opioid Addiction

BWWC
BOSTON WOMEN'S WORKFORCE COUNCIL

Pay Equity

Medical Data Sharing

Greater Boston Chamber of Commerce

Economic Inclusion

The Dataverse® Project

Social Science Research Sharing

CALLISTO

Detecting Serial Perpetrators of Sexual Misconduct

MPC FOR SOCIAL GOOD

Hey,Charlie

Combatting Opioid Addiction

BWWC
BOSTON WOMEN'S WORKFORCE COUNCIL

Pay Equity

Medical Data Sharing

Greater Boston Chamber of Commerce

Economic Inclusion

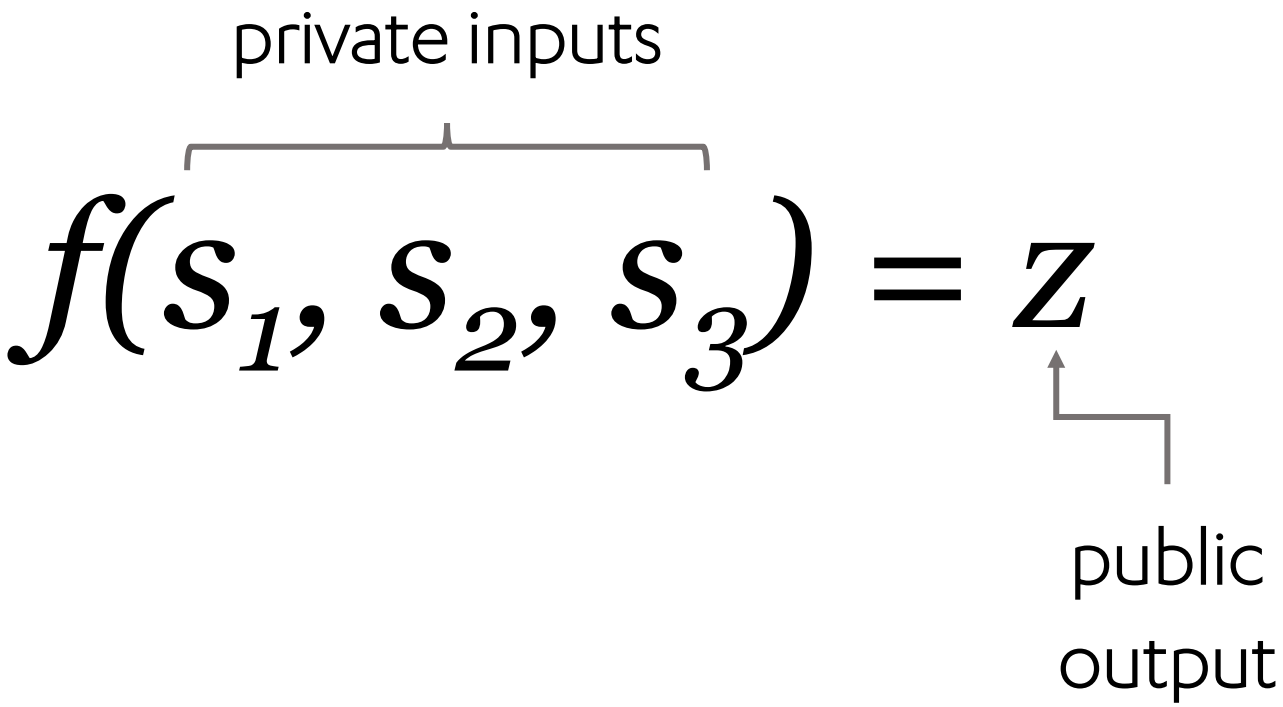
The Dataverse® Project

Social Science Research Sharing

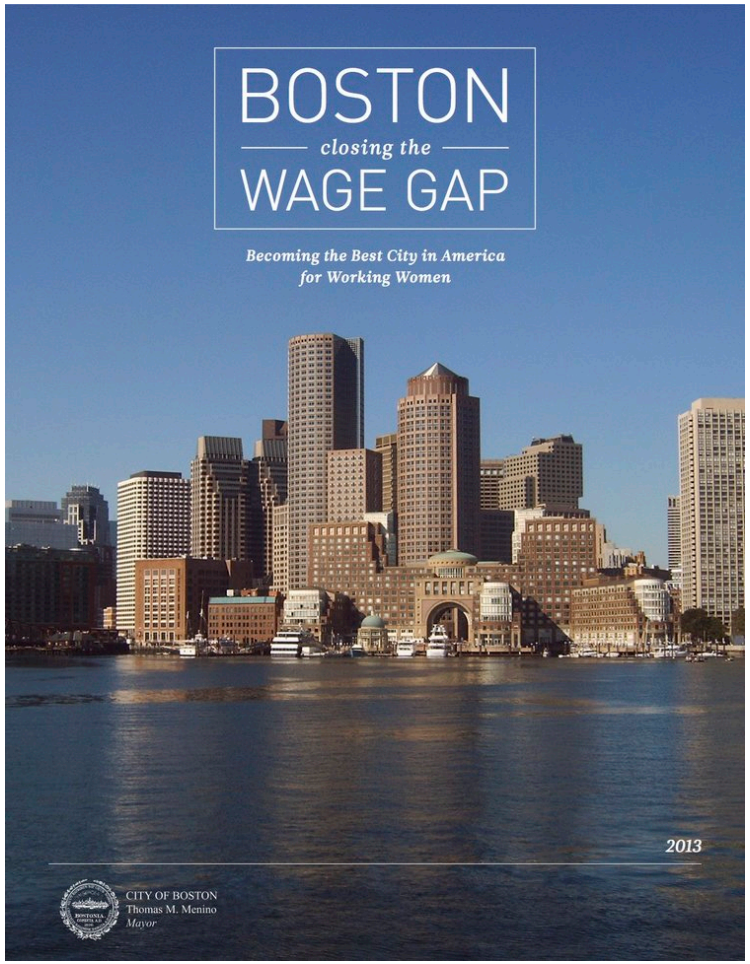
CALLISTO

Detecting Serial Perpetrators of Sexual Misconduct

SECURE MULTI-PARTY COMPUTATION (MPC)



CLOSING THE WAGE GAP IN BOSTON



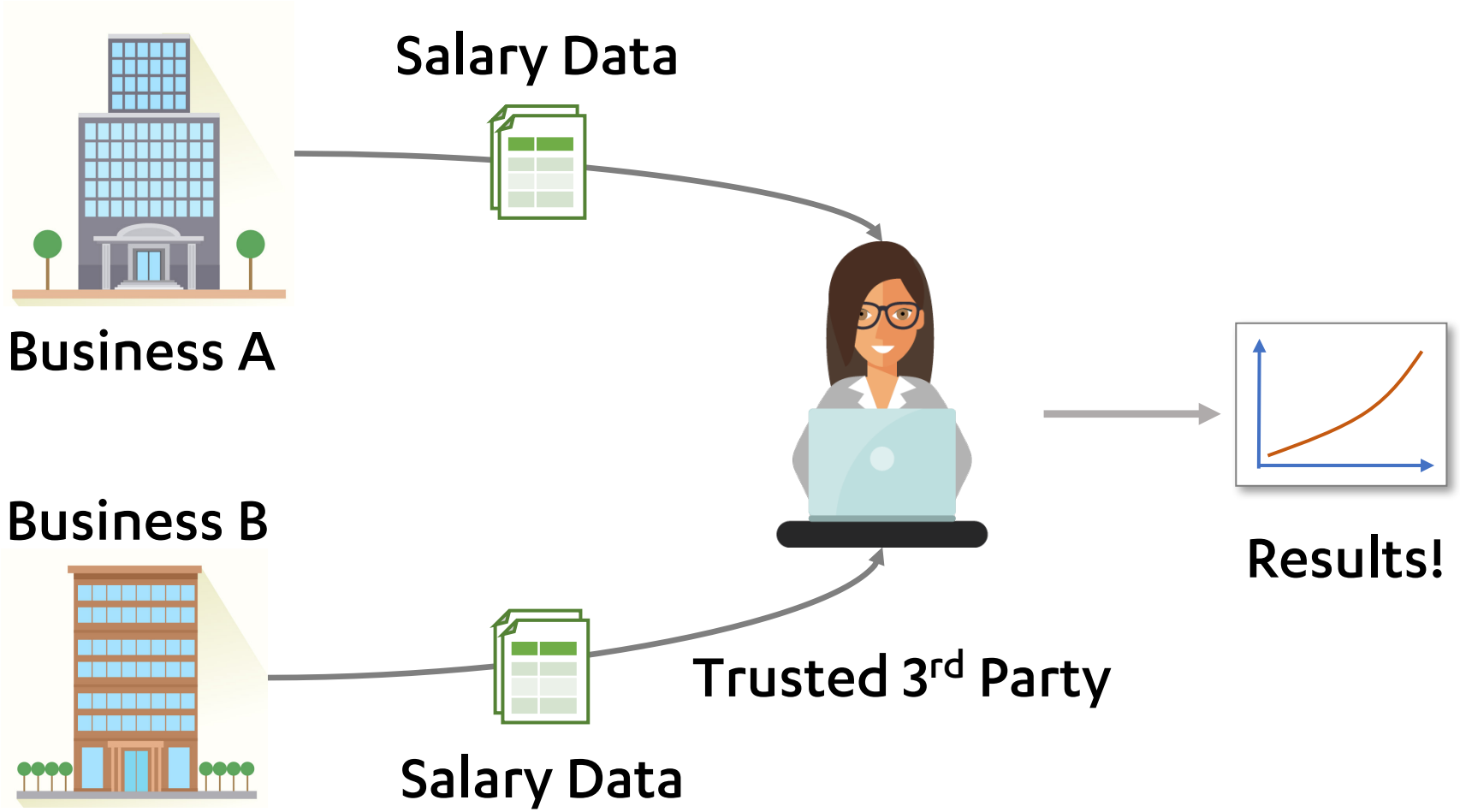
BWWC

BOSTON WOMEN'S WORKFORCE COUNCIL

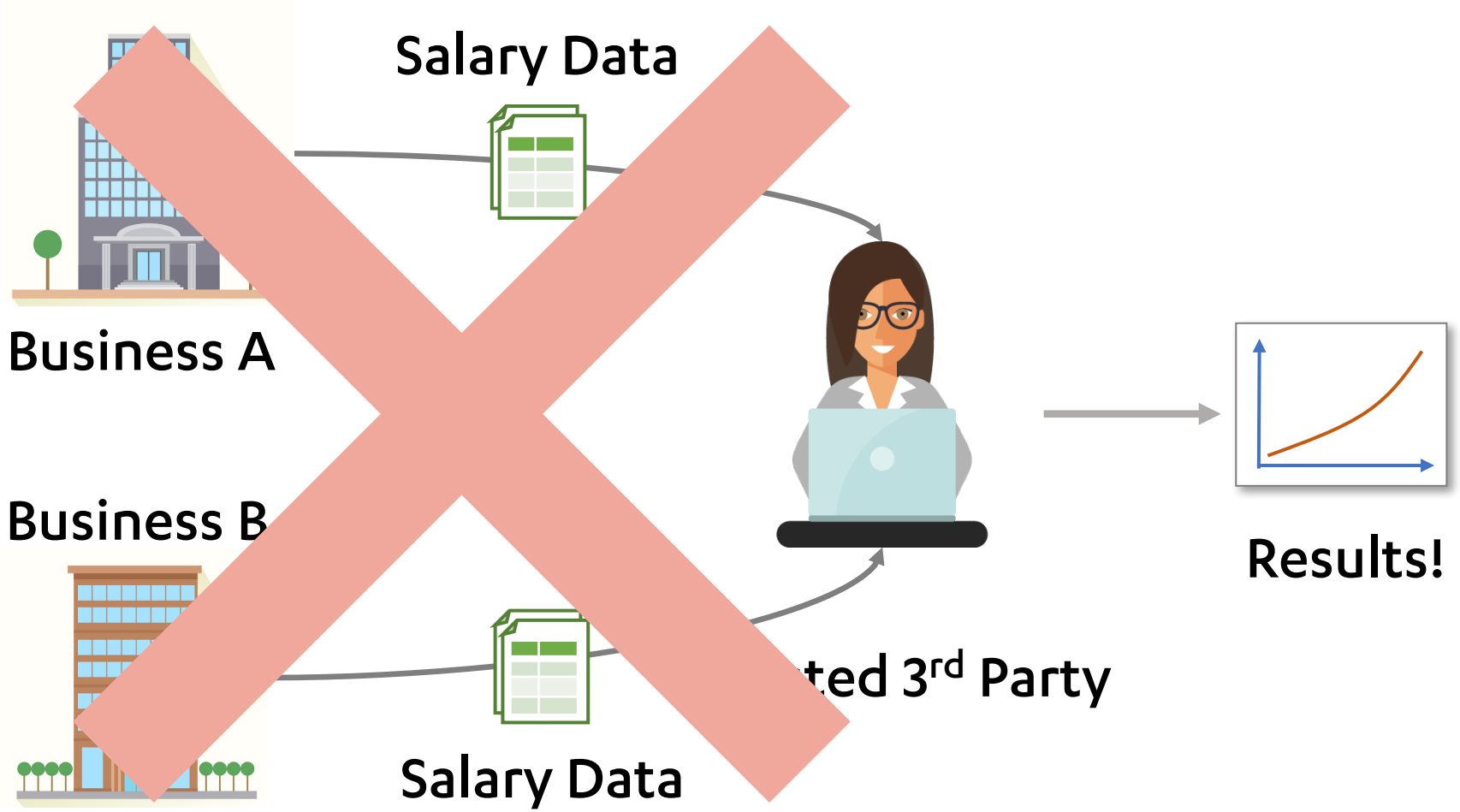
1. Understanding the root causes of the wage gap
2. Closing the gap
3. Evaluating success

Over 200 Businesses

ORIGINALLY PROPOSED WORKFLOW



ORIGINALLY PROPOSED WORKFLOW



ROLES & CONCERNS

Lawyer

BWWC

HR/Diversity Personnel

IT Personnel

ROLES & CONCERNS

Lawyer
Liability

BWWC

HR/Diversity Personnel

IT Personnel

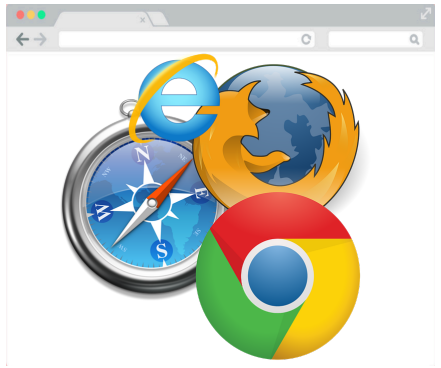
ROLES & CONCERNS

Lawyer
Liability

BWWC
Participation

HR/Diversity Personnel

IT Personnel



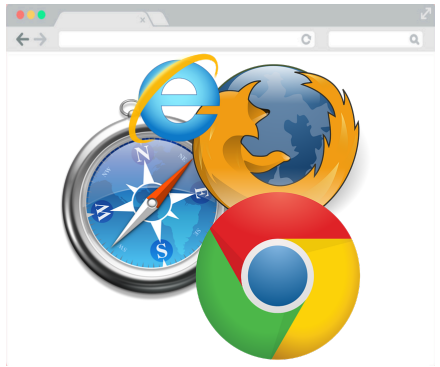
ROLES & CONCERNS

Lawyer
Liability

BWWC
Participation

HR/Diversity
Personnel
Usability

IT Personnel



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																

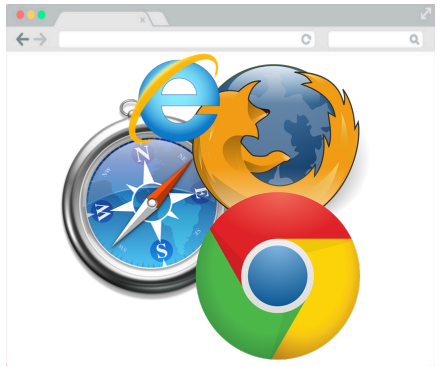
ROLES & CONCERNS

Lawyer
Liability

BWWC
Participation

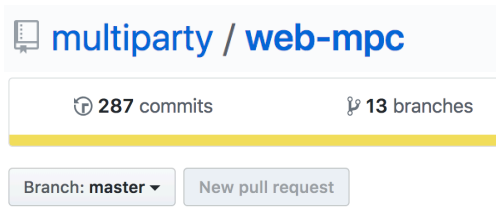
HR/Diversity
Personnel
Usability

IT Personnel
Auditability

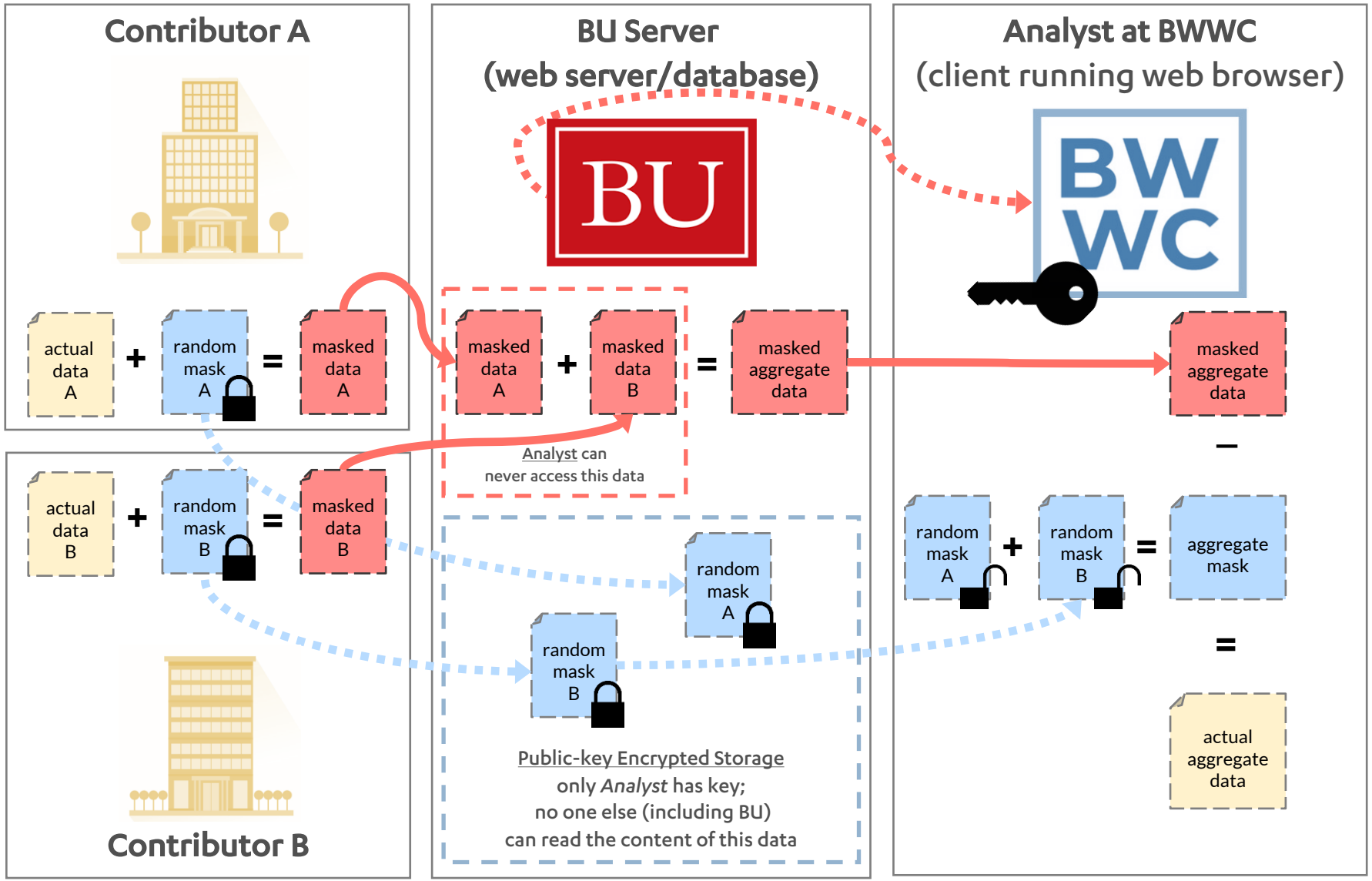


Total Annual Compensation (Dollars)

	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																



MPC SOLUTION



100talent.org

Input your data

Please make sure your session key and participation code match the ones provided in the email sent to you by the BWWC. Drag and drop your completed template file to encrypt and include your submission in the aggregate data.

Session key

Session key

Participation code

Participation code

Drag and drop your completed template file here

—or—

Choose file

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																

Submit

ERROR CHECKING

Asian		American Indian/Alaska Native		Two or More Races (Not Hispanic or Latinx)	
Female	Male	Female	Male	Female	Male
0	0	0	0	0	0
18	10000000	110	111	112	113
28	29				
38	39				
48	49	410	411	412	413

Warning: Data is too big

Are you sure this value is correct?

adfs	$47.00	$48.00	$49.00	$410.00	$411.0
$56.00					
$66.00					
$76.00	$77.00	$78.00	$79.00	$710.00	$711.0

Invalid Data Entry

Please do not input any text or leave any cells blank. If the value is zero, please input zero.

Verify and submit your data

Please ensure that all data entered is accurate, and confirm that all employees are accounted for by reviewing the total number of employees below.

Totals Check

	Total Number of Employees		
	Female	Male	All
Total	15905	16390	32295

☐ All data is verified and correct

Errors

- Invalid session number
- Invalid participation code
- Please answer all Additional Questions

Submission history

- You have not submitted yet

Submit

USER EXPERIENCE & WEB ANALYTICS

Answer additional questions

We have included these questions to get instant feedback as to how this process went in order to improve the process in future years. Please know that the answers to these questions will be anonymous, and they will be considered separately from the encrypted and aggregated data above.

Which department are you in?

- Human Resources (e.g. HR Manager, HRIS Manager, Compensation Manager, Talent & Development)
- Operations (e.g. Director of Operations)
- Diversity (e.g. Chief Diversity Officer)
- Upper Management (e.g. COO, CEO, Executive Director)
- Other

What kind of HRIS or organizational system does your company/organization use?

- Large-scale traditional HRIS/HRMS software (e.g. ADP, Workday, PeopleSoft, etc.)
- Microsoft Office or similar (e.g. Excel, Microsoft Word, Google Docs)
- Other

How easy was it to understand what data was required given the template and instructions?

- Extremely easy
- Moderately easy
- Slightly easy
- Neither easy nor difficult
- Slightly difficult

USER EXPERIENCE & WEB ANALYTICS

Answer additional questions

We have included these questions to get instant feedback as to how this process went in order to improve the process in future years. Please know that the answers to these questions will be anonymous, and they will be considered separately from the encrypted and aggregated data above.

Which department are you in?

- Human Resources (e.g. HR Manager, HRIS Manager, Compensation Manager, Talent & Development)
- Operations (e.g. Director of Operations)
- Diversity (e.g. Chief Diversity Officer)
- Upper Management (e.g. COO, CEO, Executive Director)
- Other

What kind of HRIS or organizational system does your company/organization use?

- Large-scale traditional HRIS/HRMS software (e.g. ADP, Workday, PeopleSoft, etc.)
- Microsoft Office or similar (e.g. Excel, Microsoft Word, Google Docs)
- Other

How easy was it to understand what data was required given the template and instructions?

- Extremely easy
- Moderately easy
- Slightly easy
- Neither easy nor difficult
- Slightly difficult

Answer additional questions

We have included these questions to get instant feedback as to how this process went in order to improve the process in future years. Please know that the answers to these questions will be anonymous, and they will be considered separately from the encrypted and aggregated data above.

Which department are you in?

- Human Resources (e.g. HR Manager, HRIS Manager, Compensation Manager, Talent & Development)
- Operations (e.g. Director of Operations)
- Diversity (e.g. Chief Diversity Officer)
- Upper Management (e.g. COO, CEO, Executive Director)
- Other

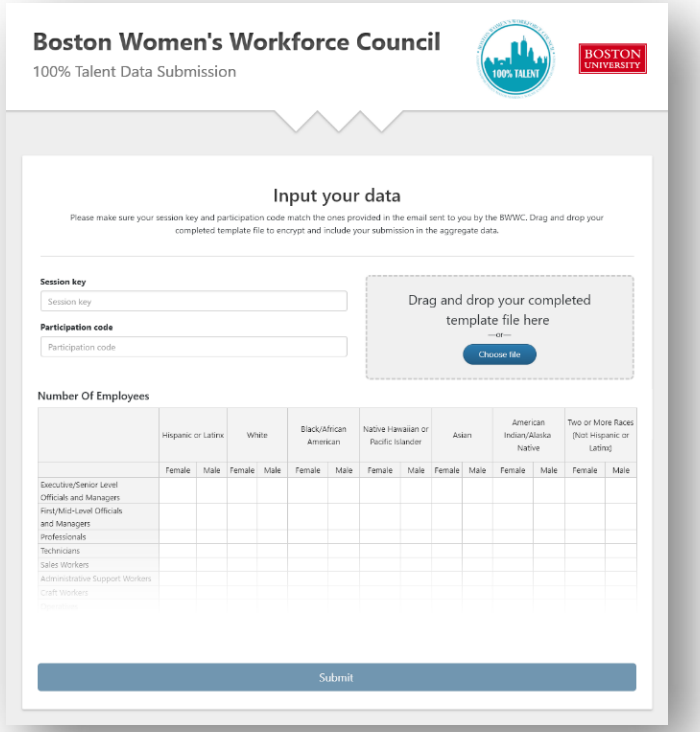
What kind of HRIS or organizational system does your company/organization use?

- Large-scale traditional HRIS/HRMS software (e.g. ADP, Workday, PeopleSoft, etc.)
- Microsoft Office or similar (e.g. Excel, Microsoft Word, Google Docs)
- Other

How easy was it to understand what data was required given the template and instructions?

- Extremely easy
- Moderately easy
- Slightly easy
- Neither easy nor difficult
- Slightly difficult

MPC ENABLED FOR DATA ANALYSIS



	2016	2017
total # of employers	69	114
# employees (1000s)	113	167
% of workforce	11	16
total annual earnings	$11b	$15b

LONGITUDINAL DATA

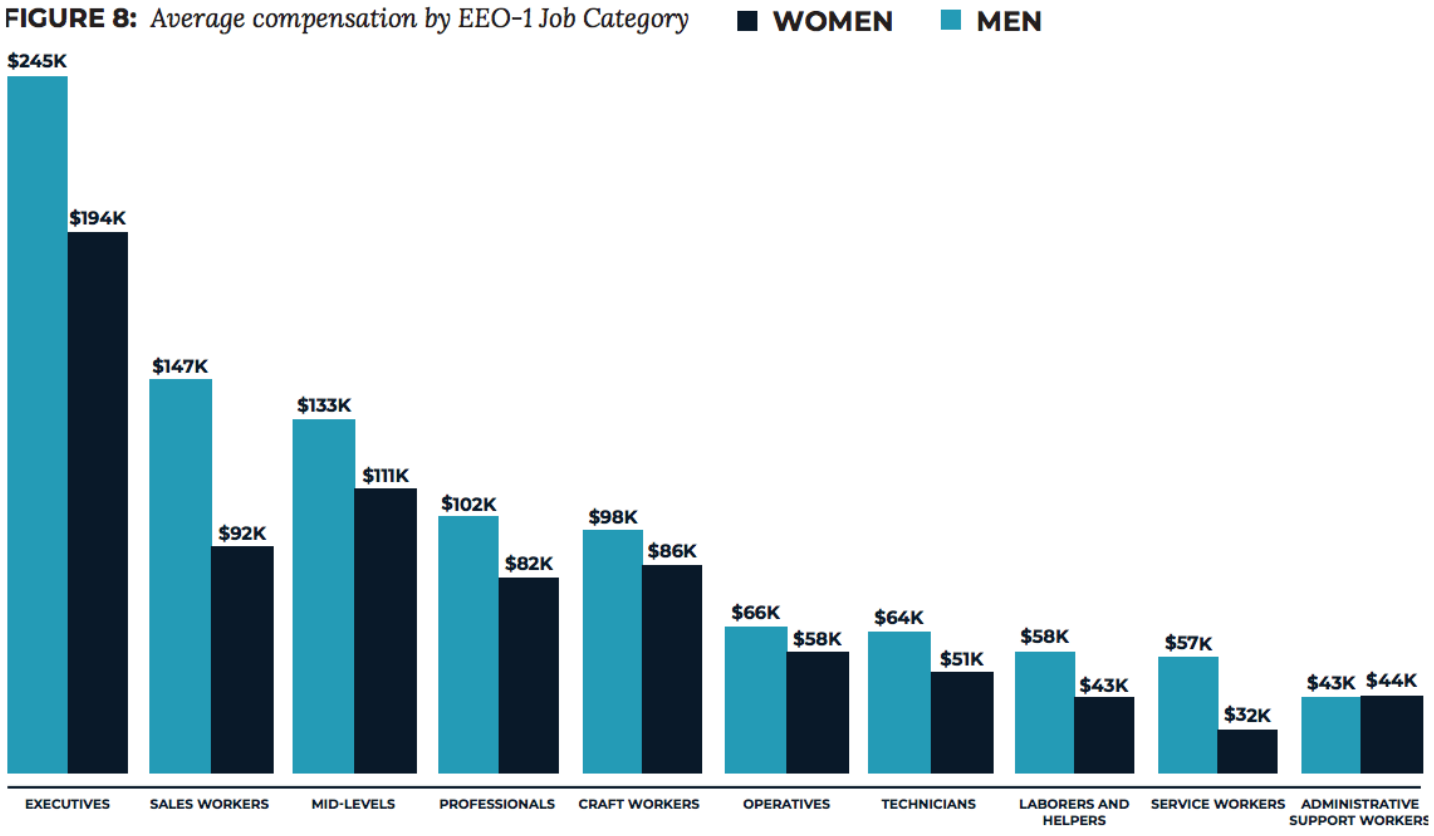
City of Boston
Women's Advancement

City of Boston
Mayor Martin J. Walsh

BOSTON UNIVERSITY

100% TALENT

IMPROVED DATA GRANULARITY



FROM DATA TO IMPACT

BOSTON WOMEN'S WORKFORCE COUNCIL

UPCOMING EVENTS

Thank you for making 2017 a success! We hope to see you at our **upcoming events in 2018/19**.

Q4 BRIEFING: WOMEN'S LEADERSHIP ORGANIZATIONS - ACADEMICS AND ACTIVISTS

DATE October 24, 2018
TIME 7:30-9:30AM

ANNUAL BEST PRACTICES CONFERENCE

DATE December 4, 2018
TIME 8:00-10:30am

Q1 BRIEFING: TECHNOLOGY GAME CHANGERS

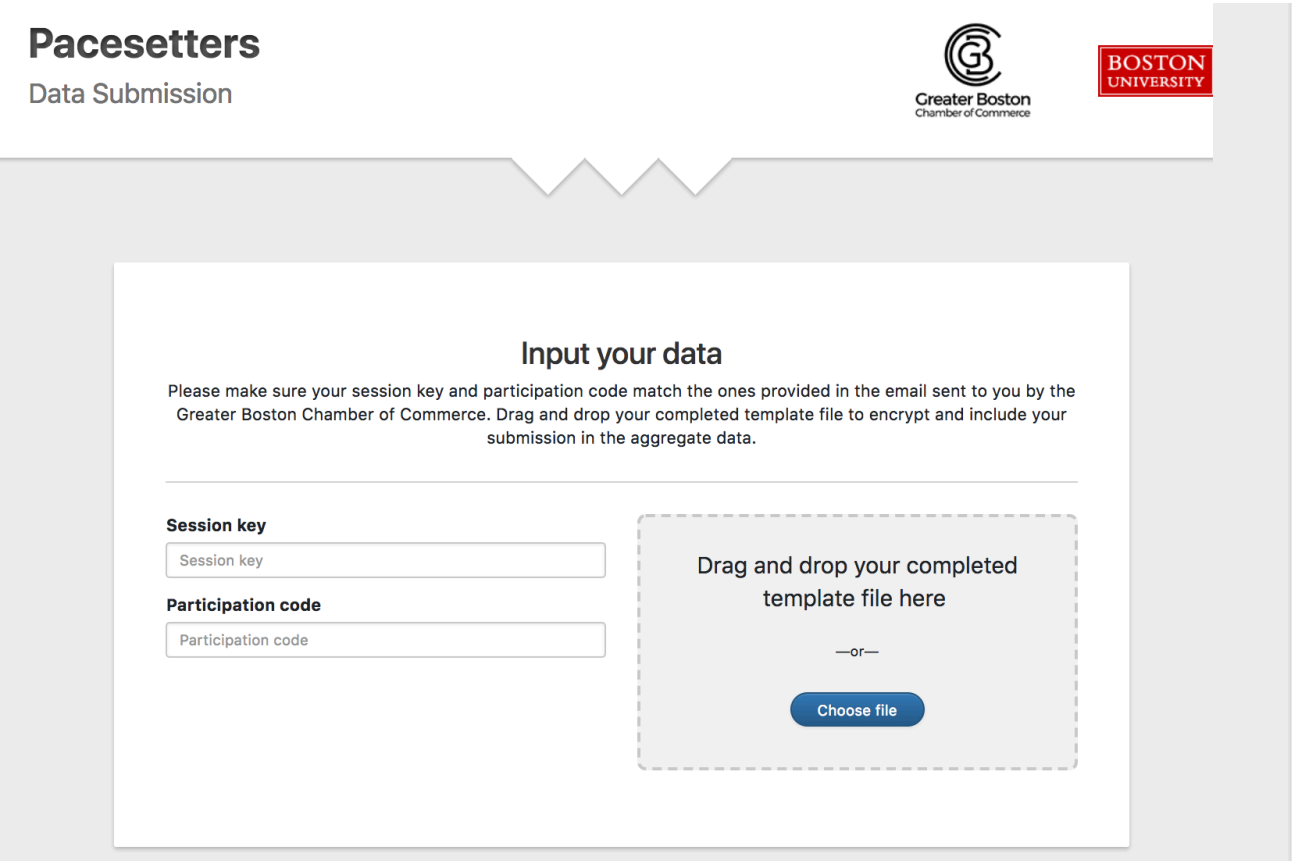
DATE January 31, 2019
TIME 7:30-9:30AM

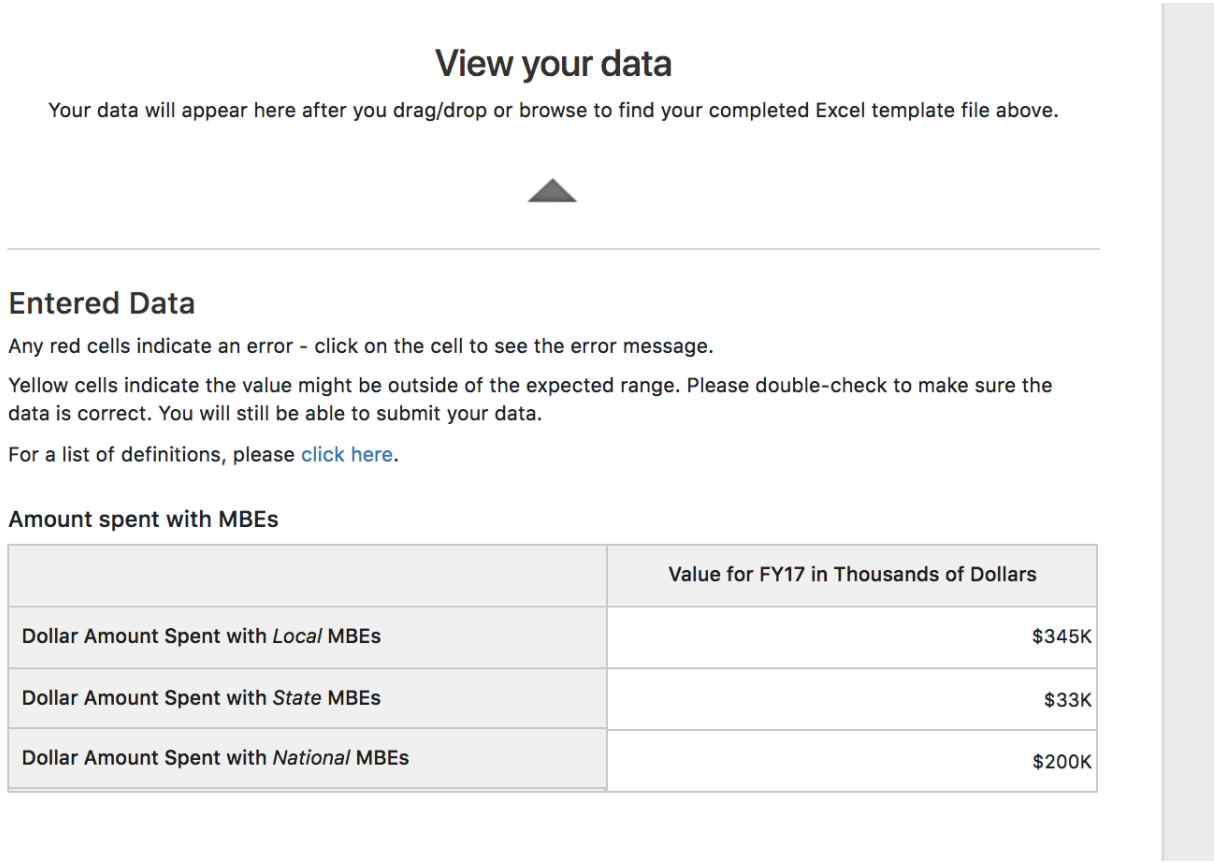
SAVE THE DATE

LOCATIONS TBD

Sign up for our newsletter on our website **bostonwomensworkforcecouncil.com** for updates!

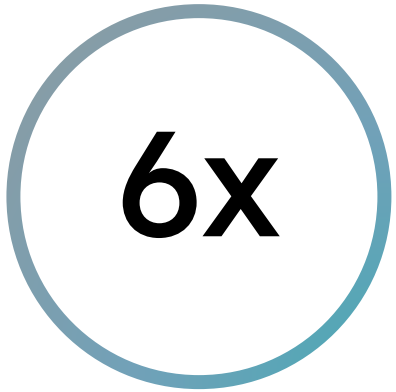
SUPPORTING LOCAL MINORITY-OWNED BUSINESSES



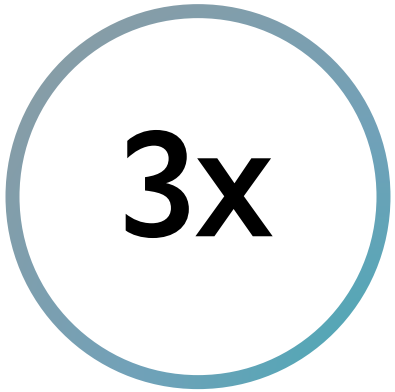


	Value for FY17 in Thousands of Dollars
Dollar Amount Spent with *Local* MBEs	$345K
Dollar Amount Spent with *State* MBEs	$33K
Dollar Amount Spent with *National* MBEs	$200K

DETECTING SERIAL PERPETRATORS OF SEXUAL MISCONDUCT



more likely to report through a school's Callisto website than to their school or the police



more likely to seek out medical and emotional support **services** after using Callisto

of survivors were **matched** with another survivor who reported the same perpetrator

CALLISTO

Identifying information about a ***survivor*** and the ***accused*** can only be decrypted by a lawyer when ***at least 2 users*** name the same perpetrator

CALLISTO

Callisto: A Cryptographic Approach To Detect Serial Predators Of Sexual Misconduct

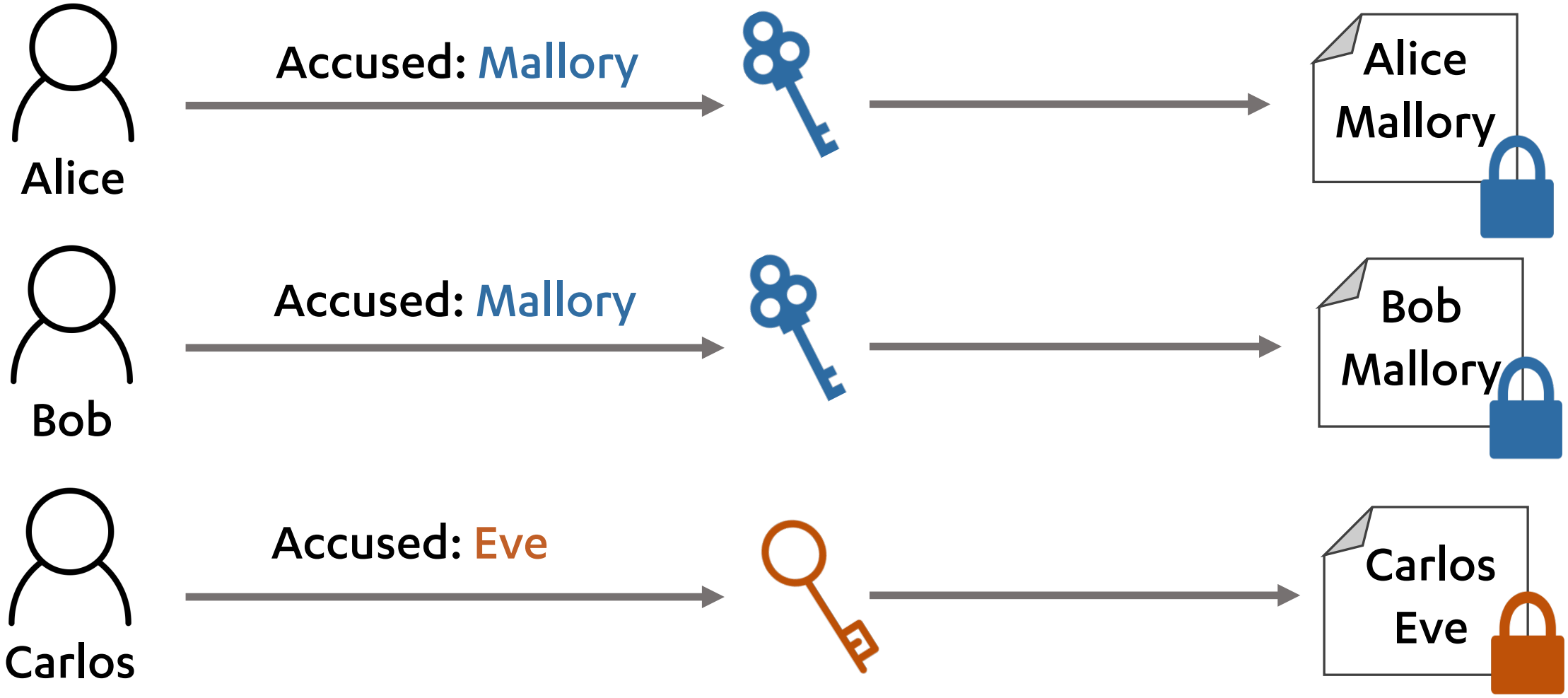
Anjana Rajan Lucy Qin David Archer
Dan Boneh Tancrède Lepoint Mayank Varia

March 29, 2018
Last updated: November 14, 2018

Abstract

Callisto, a non-profit that has created an online sexual assault reporting platform for college campuses, has expanded its work to combat sexual assault and professional sexual coercion in other industries. In our new product, users will be invited to an online *matching escrow* that will detect repeat perpetrators and create pathways to support for victims. Users of this product enter incident details and perpetrator identities into the escrow. This data can only be decrypted by a Legal Options Counselor (a third-party lawyer vetted by Callisto) when at least one other user enters the identity of the same perpetrator. If perpetrator identities match, each user is assigned a Legal Options Counselor, who will connect users to each other (if appropriate) and help each user determine their best path towards justice. User relationships with Legal Options Counselors are structured so that relevant communications benefit from client-counselor privilege. A combination of client-side encryption, encrypted communication channels, oblivious pseudo-random functions, key federation, and Shamir Secret Sharing keep data encrypted so that only Legal Options Counselors gain access to identifying user submitted data when a perpetrator match is identified. In this paper, we present an informal risk management assessment, threat model, and cryptographic solution overview for our new product. A later paper will provide a formal security analysis and mathematical proofs of our cryptographic scheme.

DETECTING SERIAL PERPETRATORS OF SEXUAL MISCONDUCT



DETECTING SERIAL PERPETRATORS OF SEXUAL MISCONDUCT

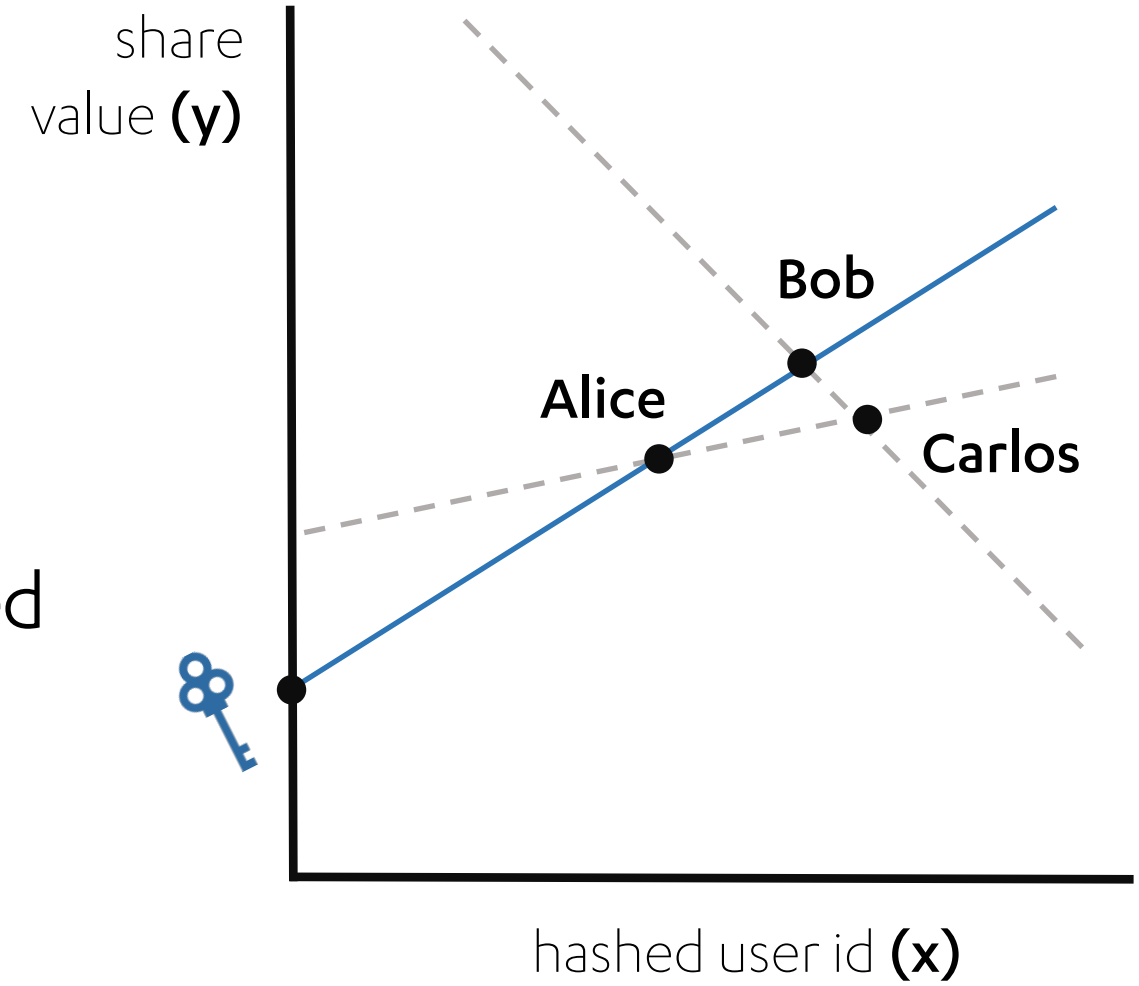
slope

$$y = ax + k$$

hashed user id

key represented as y-intercept

where ***(x, y)*** is a share



The Callisto Survivor's Guide

1. Welcome. We believe you.

Before you begin, please know that you are not alone. We have created this guide to share information and resources for survivors of sexual assault, rape, and sexual coercion. We hope that you find it helpful.

We know that this time in your life can be very stressful and that much of the language here may be triggering or upsetting. However, we also hope that you find this guide to be empowering and uplifting. It is written by fellow survivors to remind you that you are surrounded by a community of caring individuals, and that there are many resources available to help you on your journey.

User Inputs

STEP 1 | STEP 2 | STEP 3 | STEP 4 | STEP 5 | STEP 6

Our encryption method focuses on several cryptography techniques (our white paper explains these in more detail.) This demo highlights two techniques: **client side encryption** and **Shamir Secret Sharing**.

To begin, enter a user name and perpetrator name. This data will be encrypted with a record key, k'. Data inputs will not be stored.

ENTER USER NAME

ENTER PERP NAME

next

/multiparty/umbral
/multiparty/oprf

DEPLOYING MPC FOR SOCIAL GOOD

THANK YOU

multiparty.org
sail.bu.edu

/multiparty
/hicsail

@lcyqn
@bu_computing
@hicsail