Boston Regional Intelligence Center

Boston Police Department

Privacy Committee

One Schroeder Plaza

Boston, MA 02120

November 30, 2015.

PRIVACY COMPLAINT

To whom it may concern:

The Boston Regional Intelligence Center's Privacy Policy states (Section K.4.1) that *"if an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that: (a) Is exempt from disclosure, (b) Has been or may be shared through the ISE, or (c) (1) Is held by the BRIC and (2) Allegedly has resulted in demonstrable harm to the complainant"*, the individual may submit a complaint that the Privacy Policy has been violated.

I (Maya Shaffer of news organization the Bay State Examiner, www.baystateexaminer.com) have reason to believe that my privacy has been violated in the manner described above. I am submitting a formal complaint under the Boston Regional Intelligence Center Privacy Policy.

1. **Background**

I am a journalist with the Bay State Examiner, a news organization and member of the Boston Institute of Nonprofit Journalists. I was documenting the nature of the security requirements being imposed on members of the public wishing to attend the finish line of the 2015 Boston Marathon. In particular, I was concerned about the possibility of violations of the publics Fourth Amendment by the Boston Police Department, including, but not limited to, blocking public streets and requiring all members of the public, irrespective of whether there was any suspicion at all of involvement in criminal activity, to have their bags searched. Our reporting on the subject may be found at http://www.baystateexaminer.com/articles/at-2014-boston-marathon-bags-searched-without-warrants?rq=boston%20marathon , http://www.baystateexaminer.com/articles/the-terrorists-won?rq=boston%20marathon , and

http://www.baystateexaminer.com/articles/independence-day-marred-by-police-state-checkpoints.

Factual Basis for Complaint

After the 2015 Marathon, on October 24, I submitted a Public Records Request to the Boston Police Department (and Boston Regional Intelligence Center), asking for "All records related to the monitoring of Maya Shaffer, and/or the Bay State Examiner (or Baystate Examiner) including but not limited to BRIC files" . I received a response on November 16, **falsely stating** "There are no records responsive to your request."

On August 8, 2015, a BRIC Senior Analyst, Ryan Walsh, made a presentation to the National Geospatial Preparedness Summit on using geolocation data for surveillance purposes. This presentation was uploaded to the NAPSG Foundation website at http://www.napsgfoundation.org/wp-content/uploads/2015/08/Workshop_Boston_Marathon_Fusion_Center_20150804.pdf. Though the slide at issue has since been deleted from the presentation's online version, I was able to capture a screenshot from the presentation (see attached).

The slide displayed an example of the threat tracking conducted by BRIC at the 2015 Marathon. As part of the right-hand column, the section labeled "WebEOC" listed security threats in the environment of the Marathon finish line. It includes the following text:

> *"Informational Purposes Update 12:50pm*
>
> *Location is Boston Checkpoint 26 (Fairfield & Newbury, Boston)*
>
> *3 individuals from Baystate Examiner going from checkpoint to checkpoint testing security measures and filming interactions.*
>
> *They appear to be posting to Twitter as they go along.*
>
> *Dave Rodham."*

It is reasonable to believe that, under subsection (b), this constitutes information that "Has been or may be shared through the ISE." If that is correct, this complaint may proceed on that basis alone.

In the event that this information from WebEOC has not been or will not be shared through the ISE, I nevertheless also have adequate grounds under subsection (c) for this complaint to be considered by the Privacy Committee.

Dave Rodham, who is stated to having provided intelligence used in this report (or some part of the report), appears to be affiliated with MEMA, who worked with the BRIC on the 2015 Marathon security. This multiagency collaboration ran information about me through the BRIC to all of the agencies involved. Further, the slide deck from

which this slide was taken was uploaded to the NAPSG website after Ryan Walsh provided it to them, and was used in a presentation by Ryan Walsh which was billed in the NAPSG agenda (found here: http://www.napsgfoundation.org/wp-content/uploads/2015/07/FINAL_AGENDA_NGPS_2015.pdf) as "Combined Workshop and Simulation: Lessons Learned and Solutions in Applying GIS for Special Events - Ryan Walsh, Senior Intelligence Analyst, Boston Regional Intelligence Center - Boston Police Department".

This improper sharing of my private information went to (according to NAPSG's website):

"**Public Safety Officials & Emergency Responders**** - Management level & Operational public safety from all disciplines (fire, law enforcement, emergency management, health, 911-dispatch, search and rescue, fusion centers).

GIS Responders & IT Practitioners – State GIS Coordinators/GIOs, GIS Technicians, Specialists, GIS Managers, Technology Coordinators, Local CTOs, IT Specialists, Interoperability Coordinators.

Federal Agencies - FEMA, Depts. of Homeland Security, Justice, Defense, Energy, Transportation, National Guard, NOAA, DOI, etc.

Volunteers that Support Public Safety – American Red Cross, Crisis Mappers, etc.

Private Sector - Representatives & managers of companies that provide services to public safety, GIS & technology solution providers, institutions of higher education, and infrastructure owners/operators."

First Amendment Harms Resulting from Privacy Violation

The second part of subsection (c) relates to an allegation of "substantial harm".

It is beyond reasonable dispute, given the facts alleged in Section 2 above, that information was gathered, used, and disseminated on myself, and my publication, based *solely* on my First Amendment-protected activities.

There was no element of my activities on that day that was not peaceful or connected to my gathering information in order to convey information to the public. It is a matter of significant public interest to know whether the BRIC and law enforcement are adequately securing the Marathon finish line, and adequately protecting residents' rights as they do so. Mere dislike of the fact that I was lawfully asking questions about the security arrangements at the checkpoints I went to, and lawfully recording my interactions with police officers, is not sufficient for me to be lawfully reported as part of a system intended to convey security threats, and then harassed as a result of that threat

report. It is not true that I was "tweeting as [I] went along" about the security arrangements – my last tweet was just before I arrived at the event, not in the course of my on site newsgathering – and even if I had live-tweeted about the security arrangements, such activity would have been lawful and protected by the First Amendment. I invite the Privacy Committee to review my footage from that day; they will look in vain for any instance of conduct on my part that was not peaceful or not connected with my professional newsgathering purpose.

To collect information on innocent Massachusetts residents in this improper manner contravenes BRIC's own Privacy Policy, guidance from the Global Justice Information Sharing Initiative giving Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies, and 28 Code of Federal Regulations (CFR) Part 23.

3a. Violation of BRIC's Privacy Policy

Section E(2) of the Privacy Policy states plainly that *"The BRIC will not seek or retain and originating agencies will agree to not submit information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientation."* The Bay State Examiner is a *"noncriminal organization"*, and it is on the basis of our professional activities as reporters for that organization that *"information"* was *"submitted"* about us.

3b. Violation of Recommendations for First Amendment-Protected Events

The Global Justice Information Sharing Initiative's "Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies" mentions as a "Post-Event State Red Flag", *"Sharing information about the group with other justice entities."* (December 2011 version, page 4). The same document, on pages 11-12, has a list of activities by law enforcement that should be considered as "prohibited", which includes *"Investigating and collecting, maintaining, using, or sharing information regarding persons or groups solely because they are involved in constitutionally protected activity."* This document must be considered to be part of BRIC's set of policies, because it was supplied by BRIC in response to a public records request asking for their policies relating to surveillance of First Amendment-related activities. The 2015 Boston Marathon was clearly a "First Amendment-protected event" because, with the exception of riots and (under Massachusetts law) unlawful assemblies, all events are First Amendment-protected.

3c. Violations of 28 CFR Part 23

BRIC awards itself points in its 2013 Fusion Center Assessment Individual Report (the most recent copy that we possess), saying that BRIC's *"policies, processes, and mechanisms for receiving, cataloging, and retaining information (provided to the center) comply with 28 Code of Federal Regulations (CFR) Part 23 when appropriate."* If we consult the language of 28 CFR Part 23, we find that this incident substantively violated it:

> *Section 23.20: Operating Principles*
>
> *(a) A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.*
>
> *(b) A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.*
>
> *(c) Reasonable Suspicion or Criminal Predicate is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.*
>
> *(d) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this*

responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

Subsection (a) is violated here by BRIC having *"collect[ed] and maintain[ed] criminal intelligence information concerning an individual"* without *"reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity."* I clearly disclosed that I am a journalist, and BRIC as clearly understood that I am a journalist, by describing me as such in their alert. Officer Walsh therefore knew that this information lacked reasonable suspicion, but collected the information anyway, and BRIC's First Amendment-protecting measures were so grossly insufficient that they then disseminated this information proudly to other justice organizations as an example of the great things they were doing with geolocation data.

Subsection (c) is violated by treating my news organization, the Bay State Examiner, and the journalistic activities associated therewith, as being analogous to a criminal enterprise, and by BRIC's failure to assure that information it had gathered possessed a basis of reasonable suspicion of involvement in a crime.

Subsection (e) is violated by disseminating information on us to other justice agencies where there was no "need to know and a right to know the information in the performance of a law enforcement activity." There cannot have been a need to know, because it is obvious that participation by the BRIC employee in the conference presentation was discretionary, and the organizations represented in the audience had no right to know that the Bay State Examiner had been designated as a security threat. The same educational purpose could have been achieved by redacting the name of my organization, which was not done. BRIC then compounded their error by allowing the information to be made publicly accessible on the NAPSG website.

I allege that as a consequence of this illegal sharing of information, the Bay State Examiner suffers the substantial reputational harm of being considered, personally and corporately, as a security threat.

2. Physical Harms Suffered As A Result of the Privacy Violation

Beyond this, I, Maya Shaffer, state that I also suffered physical harm as a result of BRIC's information sharing. After visiting checkpoint 26, the checkpoint identified in "update", and visible in my recorded interactions with other officers, I was shoved and physically manhandled, but not before. It also appears that Sgt. Miller began following me from checkpoint to checkpoint, which was inappropriate in the utter absence of suspicion of any crime.

Sgt. Miller must have received the BRIC's notification about me because he first approached me and said without prompting (or any notification from me that I am a journalist asking about the security measures), "Any comments would have to be through media relations… if you do go through here though we do have to search your bag." Miller then appeared at the next checkpoint as well and joined in with another officer in shoving me.

3. Process and Remedies

There seems to be no doubt in this case that BRIC clearly contravened its own privacy policy; its guidance on how to handle First Amendment events; and the federal statute governing the collection, use and dissemination of criminal intelligence information. This sets a dangerous precedent for any journalists attempting to report on the activities or structures of BRIC, or on the security arrangements for large public events.

The Privacy Policy specifies that the Privacy Officer "on behalf of the Privacy Committee, will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law." BRIC cannot truthfully deny the existence of the information, because BRIC has already made it public. The Privacy Policy then states that *"All information held by the center that is the subject of a complaint will be reviewed within thirty (30) days and confirmed or corrected/purged if determined to be inaccurate, incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within thirty (30) days, the center will not share the information until such time as the complaint has been resolved."*

It is therefore clear that the Privacy Policy contemplates the possibility of purging inaccurate information. It is inaccurate to have collected, to retain, and to disseminate information on my journalistic activities at the 2015 Boston Marathon in a context that

in any way suggests that it was criminal or inappropriate for me to engage in my profession in this manner.

I am therefore requesting that the Privacy Committee take the following steps to remedy these violations:

(1) Purge from all BRIC systems, and take steps with partners to purge from their systems, any Suspicious Activity Reports, tips, lead information, watchlist designations, or other information that implicitly or explicitly treats the Bay State Examiner or myself, Maya Shaffer, as a threat, security risk, or suspicious or subversive person or organization, or any other adverse information, in connection with my activities at the 2015 Boston Marathon.

(2) Review any other information on the Bay State Examiner, Maya Shaffer or my colleague Andrew Quemere, stored in BRIC systems or partner systems, to ensure that no information has been collected, retained, used or disseminated in connection with these organizations or individuals that is not based on individualized probable cause of involvement in past, actual, or planned criminal activity. Neither of us have ever been charged with any criminal act.

(3) Conduct a random audit of a percentage of BRIC's criminal intelligence information, to review whether other organizations or individuals have also improperly been included in BRIC's or partner systems, and take steps to purge that information as appropriate. We believe that, as recommended in reform proposals in the Boston legislature, conducting this process annually would be appropriate.

(4) Review the process by which BRIC responds to Freedom of Information Act requests, to ensure that what is communicated to inquiring members of the public is wholly truthful, and is as complete as possible without posing a genuine and imminent danger to national security. As part of this process, we are requesting that an Internal Affairs complaint be opened against the records custodian, who falsely claimed to us that the Boston Police Department did not possess the requested records.

(5) In that spirit, to communicate truthfully with us as to the actions you have taken, and what you have found out as a result. We request that you specify the kinds of records that were created involving us, release their text to us, and also specify the agencies to which that information was transmitted.

4. Conclusion

As far as we know, this will be the first occasion on which the mechanisms outlined in the Privacy Policy have been set into action. It is a perfect opportunity for BRIC to address significant public criticisms of opacity, unaccountability, bias, and over-focus on investigating peaceful First Amendment activity. By taking such steps, and making it known that you have taken them, you would go far to restore your reputation, in the course of repairing the damage you have done to ours.

Sincerely,

Maya Shaffer,
The Bay State Examiner
Email: BayStateExaminer@gmail.com