SURVEILLANCE TOOLKIT: CHECKLIST FOR ASSESSING A SURVEILLANCE USE POLICY

There should be enforceable written rules for every type of surveillance technology used by a government agency. The following checklist is designed to help you assess whether a written surveillance use policy meets the bare minimum requirements for protection of civil rights and civil liberties. As you review a written policy, look for shortcomings, omissions, or vague language that you can highlight for decisionmakers and in other advocacy.

SURVEILLANCE USE POLICY CHECKLIST		
Purpose of the technology	Does the policy list the specific purpose(s) of that type of surveillance technology?	**YES/NO**
Specific authorized & prohibited uses	Does the policy specifically explain the scenarios or circumstances when the agency may use the surveillance technology?	**YES/NO**
Data that can be collected	Does the policy specifically say what information the technology can be used to collect?	**YES/NO**
Data access instructions/ restrictions	Does the policy specifically say who can access or use any collected information, and under what conditions?	**YES/NO**
Data protection	Does the policy describe safeguards that protect information from unauthorized access, such as encryption, user login controls, or employee access limits?	**YES/NO**
Data Retention	If data is collected and recorded/retained, does the policy state how long collected data may be retained?	**YES/NO**
Public Access	Does the policy describe how members of the public, including criminal defendants, can access information about the technology and its use?	**YES/NO**
Third party data sharing	Does the policy specifically say whether and/or how non-City/County entities may get access to information collected with this technology? If yes, are there restrictions on that access?	**YES/NO**
Training	Does the policy describe what training is required for officers or employees who will use the technology or access the data?	**YES/NO**
Auditing and oversight	Does the policy describe how use of the technology and data will be audited, such as internal recordkeeping, automated process, or third party oversight?	**YES/NO**
Legally enforceable	Does the policy set forth consequences for misuse? Are they enforceable in a court or via a lawsuit?	**YES/NO**