

## NaCTSO Guidance Note 9/2016

### Street View Imagery/3D Imagery Mapping

#### **Introduction.**

This guidance note provides advice to business and industry regarding requests from Street View Imagery/3D Imagery companies to photograph and map the internal footprints of publicly accessible sites.

This advice is **not** written to discourage use of imagery, but to provide some consideration of the security implications and value that this tool could provide to a person with criminal intent.

Corporate and personnel digital footprints can allow a terrorist or criminal with hostile intent to potentially obtain significant information that may assist in preparing an attack, protest or criminal act. The accessibility of publicly available internal imagery could add to attack planning capability if reasonable mitigation measures are not considered or implemented.

#### **Mitigation Considerations.**

Prior to any attendance at the site by an imagery company to conduct photography, and having conducted due diligence checks on the company, a site should consider having some or all of the following measures agreed within the contract:

1. Agreement that all static and un-domed CCTV cameras be pixilated out of the image. (This withdraws the ability to determine CCTV type or direction)
2. Agreement that all public/back of house access control measures be pixilated. This should include any electrical or mechanical measure and must include any external access control measure to car parks or delivery entrances. If a site has installed HVM measures these should **not** be pixilated as they will add to the visible robustness of the site **but** the electrical and mechanical measures associated with them should be obscured.
3. Agreement that the time of the photography is determined by the site owner. The best time to have their site photographed. would be during quieter periods of the site operation. This would deny a hostile the option of determining potential casualty impact that any attack could achieve.
4. Agreement that photography be restricted to public areas only.

*Protect yourself your staff your business and your community.*

Following on from any contract agreements a site can also consider some of the following advice to enhance its digital look and feel to discourage attack planning:

Stage Management:

1. Consider the placement of your overt security teams at key points during the capture of imagery. It is recommended that the faces of staff are pixilated. Areas to consider would be at entrances (to enhance the impression of the security regime) and front of house/back of house access areas.
2. Placement of positive customer care and security posters and messages.  
<https://www.cpni.gov.uk/advice/Personnel-security1/Employee-vigilance/>

Engagement:

1. Have security staff and customer service agents being photographed in positive engagement scenes with customers. To a potential attacker this will indicate that approaches and interaction is made with customers and is again discouraging to them.
2. If the site has an onsite Police team, then photographs of joint security/police patrolling should be encouraged.

This advice is not intended to be prescriptive but to guide to reasonable mitigations to reduce any security implications.

The decision to allow the imagery activity to take place is a matter for the site owner

*Protect yourself your staff your business and your community.*

Guidance Note 9			
Title	Street View Imagery/3D Imagery Mapping	Chapter/Annex	
NaCTSO SPOC	Mike Pearce NaCTSO	Region	NCTPHQ
Subject Matter Experts			
Relevant Standard			
Additional guidance or reference material			
Link to where original documents are stored			
Quality Assurance Sign off NaCTSO			
Date Review Completed			
Next Review Date			
Completed form to be sent to website manager via <a href="mailto:NaCTSO@cpni.gsi.gov.uk">NaCTSO@cpni.gsi.gov.uk</a>			
Comms sign off			

*Protect yourself your staff your business and your community.*