Appendix

Re points 8/ & 9/ above (my bold, and comments in italics):

8/ Regulation of Investigatory Powers Act 2000

Quotes from **David Kitson's email**:

He says:

> "**Under Part 1 of RIPA** the Council's email system is categorised as a 'private telecommunication system', in that it is not a telecommunication system offered or provided to the public, but is connected to such a system.
>
> **Section 1(2)** of RIPA states:
>
> It shall be an offence for a person-
>
> (a) intentionally and without lawful authority, and
>
> (b) otherwise than in circumstances in which his conduct is excluded by subsection **(6)** from criminal liability under this subsection, to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a private telecommunication system.
>
> **Section 1(6)** of RIPA states:
>
> The circumstances in which a person makes an interception of a communication in the course of its transmission by means of a private telecommunication system are such that his conduct is excluded from criminal liability under subsection (2) if -
>
> (a) he is a person with a right to control the operation or the use of the system; or (b) he has the express or implied consent of such a person to make the interception.
>
> **Therefore no offences are being committed."**

*No **criminal** offence, perhaps, but he singularly fails to mention **Section 1(3):***

> **(3)** Any interception of a communication which is carried out at any place in the United Kingdom by, or with the express or implied consent of, a person having the right to control the operation or the use of a **private** telecommunication system **shall be actionable at the suit or instance of the sender or recipient, or intended recipient, of the communication if it is without lawful authority** and is either—
>
> (a) an interception of that communication in the course of its transmission by means of that private system; or
>
> (b) an interception of that communication in the course of its transmission, by means of a public telecommunication system, to or from apparatus comprised in that private telecommunication system.

*Note "**actionable** … if it (the interception) is **without lawful authority".***

He goes on:

"Section 1(5) of RIPA **(so far as is relevant)** states:

Conduct has lawful authority for the purposes of this section **if, and only if-**

(a) it is authorised by or under **section 3 or 4;**

(b) it takes place in accordance with a warrant under S5

… and conduct (whether or not prohibited by this section) has lawful authority for the purposes of this section by virtue of paragraph (a) or (b) shall also be taken to be lawful for all other purposes."

***Section 1 (5)** is **absolutely relevant to lawful interception** – it is misleading to suggest it isn't.*

Further, he states:

"Section 3 of RIPA provides authorisation in a number of defined situations. **Of relevance** is the following at section **3(3):**

Conduct consisting in the interception of a communication is authorised by this section if-

(a) it is conduct by or on behalf of a person who provides a postal service or telecommunications service; **and**

(b) it takes place for **purposes in connection with the provision or operation** of that service .."

*How can the interception of a personal email be in any way connected to the "provision or operation" of the service? **Section 3(3) is irrelevant.***

Section 3** is crucial – but it is the **preceding sub-sections (1) and (2), which Mr Kitson fails to note, that are relevant:

"Lawful interception ...

(1) Conduct by any person consisting in the interception of a communication is authorised by this section if the communication is one which . . . is **both—**

(a) a communication **sent by a person who has consented** to the interception; **and**

(b) a communication **the intended recipient of which has so consented**.

(2) Conduct by any person consisting in the interception of a communication is authorised by this section if—

(a)the communication is **one sent by, or intended for, a person who has consented** to the interception; **and**

(b)**surveillance by means of that interception has been authorised under Part II.**

*(1) is not applicable since clearly email interceptions have taken place without the knowledge of either the sender or recipient; any interception - to be lawful - must therefore be authorised at (2) by one party **AND** under Part II of the Act.*

In addition, Mr Kitson purports:

> "Part 1 of RIPA deals with Communications. **Part 2 of RIPA** deals with Covert Surveillance and **is not relevant to the matter at hand**."

*As demonstrated, it is. Interception of personal emails in Part II is regarded as **covert - "directed surveillance"** - and, from 2012, would require not only the consent of either sender or intended recipient but the additional authorisation of a magistrate.*

Mr Kitson concludes:

> "**In consequence of the above**, the Council (being a provider of a private telecommunications system and a telecommunications service **in order to access and make use of that system**) is able to undertake **the basic redirection of emails from unreasonable complainants."**

Non sequitur.

9/ The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

David Kitson describes the Regulations which are provided for in Section 4 of RIPA:

> "The Regulations allow a business (which includes a public authority) to intercept a communication for various prescribed purposes, including for the purpose of monitoring to prevent or detect crime, to investigate or detect unauthorised use of the system, or to secure the effective operation of the system."

It would seem, however, that Mr Kitson is using legislation enacted for entirely other circumstances to justify SBC's 'monitoring' activities. The 2000 regulations have been superseded during 2018, but there is little material difference.

*Here is a quote from the House of Lords **Hansard, at Column 1712,** during a debate earlier this year on the new regulations - the "Act" refers to the **Investigatory Power's Act**, which is replacing RIPA 2000 – (my bold):*

> "**As under pre-existing law**, the Act makes it a criminal offence to intercept communications in the absence of lawful authority. It also makes it clear that **lawful authority includes interception by businesses or other bodies where it is a legitimate practice.** These regulations set out what conduct that includes. Such activities might be, for example, call centres recording telephone calls for training purposes, companies scanning their computer networks to detect cyber attacks or businesses ensuring that their systems are not being used

for unauthorised purposes. These regulations simply ensure that companies can undertake **these important routine activities without falling foul of the offence of unlawful interception."**